APPLICATION OF GAME THEORY TO IMPROVE THE DEFENSE OF THE SMART GRID

THESIS

Keith J. Ross, Captain, USAF

AFIT/GCO/ENG/12-10

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GCO/ENG/12-10

APPLICATION OF GAME THEORY TO IMPROVE THE DEFENSE OF THE SMART GRID

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science

Keith J. Ross, BS, MA

Captain, USAF

March 2012

AFIT/GCO/ENG/12-10

APPLICATION OF GAME THEORY TO IMPROVE THE DEFENSE OF THE SMART GRID

Keith J. Ross, BS, MA
Captain, USAF

Approved:

// Signed //	2 March 2012
Kenneth M. Hopkinson, PhD (Chairman)	Date
// Signed //	17 February 2012
Meir Pachter, PhD (Member)	Date
// Signed //	2 March 2012
Timothy H. Lacey, PhD (Member)	Date

AFIT/GCO/ENG/12-10

Abstract

This thesis presents the development and evaluation of a distributed agent based system using reputation based trust and game theoretic techniques to improve the defense of the future smart grid enabled power grid from cyber-attack and equipment malfunctions. Future smart grid capabilities promise to leverage modern network technologies to revolutionize the production, transmission, distribution and consumption of electrical power. However, the internet like communication technologies also increase the power grid's vulnerability to cyber-attack. This thesis uses computer simulation linking dynamic power systems with realistic communication networks to demonstrate the benefits of a Distributed Decision Making Communication Enable Special Protection System (SPS) using reputation based trust and game theory to protect the power grid from malicious and non-malicious malfunctions. The simulations show that a distributed approach to SPS load shedding successfully maintains power grid stability after a significant electrical disturbance while using reputation based trust to defend the load shedding action from cyber-attack and equipment malfunction. Additional simulations demonstrate the successful application of game theory to strategically defend the SPS load shedding process when available resources prevent the monitoring and defense of every part of the power grid. The added capability demonstrated increases the resiliency of the power grid by preventing uncontrolled blackouts through detection and mitigation of network based attacks, therefore improving the system's reliability.

AFIT/GCO/ENG/12-10

For my wife and children who continue to sacrifice so that I can continue to serve.

Acknowledgments

I would like to express my sincere appreciation to my research advisor, Dr. Kenneth M. Hopkinson and my committee members, Dr. Meir Pachter and Dr. Timothy H. Lacey, for their guidance, feedback and support throughout the course of this thesis effort. I would also like to thank the Air Force Office of Scientific Research for sponsorship and support of this research effort.

Additionally, I am thankful for the many professors and fellow students who gave their time and effort to develop the knowledge and experience required for this type of research. Special recognition and thanks goes to Major Jose Fadul and Mr. Patrick Copeland for establishing the foundation required to go forward in this area of research. Finally, special thanks go to Lt Col Brett Borghetti, Lt Col Jeffrey Humphries, Major Hemmes, Major Ryan Thomas, Major Jonathan Butts, Dr. Rusty Baldwin, Dr. Barry Mullins, Mr. Charles Powers, Mr. Bruce Carter and Ms. Janice Jones.

Keith J. Ross

Table of Contents

Page

Page

Page

List of Figures

Page

List of Tables

Page

APPLICATION OF GAME THEORY TO IMPROVE THE DEFENSE OF THE SMART GRID

Introduction

1.1 Background

Imagine the United States without reliable power, clean water, natural gas, automobiles, electronics or any of the manufactured goods most Americans take for granted. These and many other aspects of the American society are made possible and affordable by the development and use of Supervisory Control and Data Acquisition (SCADA) Systems. SCADA systems vary from small systems encompassing a simple manufacturing process to utility systems spanning a continent. SCADA systems have improved the reliability and cost of nearly every product or utility people rely on today. [1] [2] [3] [4]

The migration of SCADA systems to the internet or internet-like networks, systems and processes realized additional increases in efficiency and cost savings. However, the further increases in efficiency and cost savings also result in a rise in the number of threats and vulnerabilities to the systems Americans take for granted. [2] [4] [5] Realizing the increased threats and vulnerabilities, President Clinton issued the Presidential Policy Directive 63 identifying the need to protect our nation's critical infrastructures. [6] The Department of Homeland Security further defined critical infrastructures with the Homeland Security Policy Directive 7, setting up a framework for better identifying vulnerabilities, threats and solutions for securing the nation's infrastructures. [7] Table 1 identifies the 17 areas identified as critical infrastructures.

Table 1. US Homeland Security, HSPD-7 Defined Critical Infrastructures [6] [7]

Critical Infrastructure / Key Resources Sectors	**Federal Sector-Specific Agency Lead (SSA)**
Agriculture and Food	Department of Agriculture and Department of Health and Human Services
Banking and Finance	Department of the Treasury
Chemical	Department of Homeland Security
Commercial Facilities	Department of Homeland Security
Commercial Nuclear Reactors, Materials and Waste	Department of Homeland Security
Dams	Department of Homeland Security
Defense Industrial Base	Department of Defense
Drinking Water and Water Treatment Systems	Environmental Protection Agency
Emergency Services	Department of Homeland Security
Energy	Department of Energy
Government Facilities	Department of Homeland Security
Information Technology	Department of Homeland Security
National Monuments and Icons	Department of the Interior
Postal and Shipping	Department of Homeland Security
Public Health and Healthcare	Department of Health and Human Services
Telecommunications	Department of Homeland Security
Transportation Systems	Department of Homeland Security

1.2 Motivation for Research

Recent events highlight the vulnerabilities of the SCADA systems and critical infrastructures that rely on the SCADA systems. Media reports revealed examples of currently operating SCADA system using hardcoded passwords that circulated on-line for years. [8] In one of the first documented attacks on a SCADA system, the Stuxnet attack on the systems controlling aspects of Iran's nuclear development reveal significant vulnerabilities. [9] Although the full effects of the Stuxnet attack have not been revealed, many believe the attacks set Iran's nuclear program back by years. [10]

As one of the identified critical infrastructures, the power grid's development into the smart grid provides an opportunity to revolutionize the production, transmission, distribution and consumption of power. This evolution involves significant expansion of the SCADA systems currently used to control the power grid. Even as smart grid technologies promise to increase the capabilities of the power grid, the network centric development of the smart grid increases the vulnerability of the power grid to attack. Reports of smart grid technologies failing to employ prudent security practices raises additional concerns. [11] News of increasing cyber-attacks on the developing smart grid along with successful demonstrations of cyber-attacks against power generators provides significant incentive to increase the security and protection of the developing smart grid. [12] [13] The threats and the examples of successful attacks on the smart grid motivate this research.

1.3 Research Focus

This research focuses on increasing the security and the protection of the evolving smart grid. Specifically, this research continues the investigation of a communication enabled agent based approach for a Special Protection Systems (SPS). A traditional SPS is a system that seeks to prevent undesirable power outages produced by power disturbances. The research begins by investigating a communication enabled agent based SPS using reputation based trust with a decentralizing SPS decision making process rather than a centralized strategy decision process while dealing with possible cyber-attacks against the SPS agents. Next, the research investigates a process for overcoming communication losses potentially created by malfunctions or cyber-attacks along with attacks on the SPS agents. Finally, this research continues by investigating the application of game theory to strengthen the SPS security and protection strategy when the SPS and the cyber-attacker are faced with limited resources.

The inspiration to apply game theory to the defense of the smart grid SPS comes from recent examples of game theory applications to improve the performance and reliability of Cognitive Radios and network defense. In the development of Cognitive Radios, game theory allows radios operating as part of a network to maximize the performance characteristics of the network through strategic power and frequency spectrum selections. [14] In the development of network defense, game theory principles help determine the optimal sampling locations, sampling rates and routing to maximize the minimum probability of detecting malicious traffic given an attacker attempting to minimize the maximum probability of detection. [15]

1.4 Organization

The remaining chapters of this thesis present the development and testing of a communication enabled SPS utilizing game theory and reputation based trust to determine a distributed strategy that mitigates the effects of a significant disturbance in a power grid while operating through a malfunction or cyber-attack. Chapter II reviews the basic concepts and current research in the areas of cyber threats and SCADA system development. The chapter then focuses on the foundation and development of the future smart grid and reviews the importance of developing reliable SPSs. Finally, Chapter II introduces trust and game theory fundamentals used to develop an agent based communication enabled distributed decision making SPS that operates reliably when experiencing malfunctions or cyber-attack.

Chapter III and Chapter IV describe the methodology used to test the agent based SPSs. Chapter III focuses on the methodology for assessing new approaches for developing an agent based distributed decision making process using reputation based trust while operating with background traffic, communication disruptions and disrupted agents. Chapter IV focuses on the methodology for assessing the application of game theory principles to an agent based distributed decision process using reputation based trust while operating with uncertainty in the reputation based trust mechanism, background traffic, communication disruptions and disrupted agents.

Chapters V and VI present and analyze the experimental results as each of the SPSs operate in simulation. The goal is to determine the success or failure of each of the revised SPSs to properly react to system disturbances while experiencing malfunctions or cyber-attack. Finally, Chapter VII summarizes this research, the contributions of the research to the development of future smart grid SPSs and suggests future research opportunities to improve SPSs.

II. Literature Review

The purpose of this chapter is to provide a brief overview of cyber threats, Supervisory Control and Data Acquisition (SCADA) systems, smart grid concepts, trust management principles, game theory fundamentals and previous centralized decision making communication enabled based Special Protection System (SPS) research. This chapter reviews basic cyber threats and areas of concern. This chapter introduces basic SCADA terminology and discusses some of the vulnerabilities and limitations when integrating SCADA systems into traditional Information Technology (IT) networks. Next, the chapter provides an overview of smart grid concepts and briefly describes new capabilities and vulnerabilities created by the transition of the nation's power grid to smart grid systems. The chapter then introduces trust management concepts. Next, the chapter briefly describes several game theory principles and illustrates possible applications of game theory principles to protect smart grid systems from malfunctions or malicious actions. The chapter concludes by describing previous research that provides the foundation for building a distributed decision making communication enabled SPS and for applying game theory to improve the defense of the smart grid.

2.1 Cyber Threats

The first step in understanding cyber related threats is to developing a common definition for cyber. Dictionary.com defines cyber as:

> *A combining form meaning "computer," "computer network," or virtual reality," used in the formation of compound words (cybertalk, cyberart, cyberspace) and by extension meaning "very modern"* [16]

To increase the precision of cyber, cyber in this research refers more specifically to cyberspace. The National Military Strategy for Cyberspace Operations defines cyberspace as:

> *A domain characterized by the use of electronics and electromagnetic spectrum to store, modify, and exchange data via networked system and associated physical infrastructures.* [17]

From these two definitions, the use of the word cyberspace covers a very broad range of systems and technologies. The rest of this research will concentrate on a narrower portion of cyberspace concerned with networks and some of the systems that rely on networks to operate.

A cursory review of cyber related news reveals several threats facing system operating in cyberspace. Recent history is full of examples of attacks against networks and networked computer systems. Very little time passes before another example of a successful attack appear in the news. In just one week, recent protests over proposed anti-piracy legislation in the United States resulted in several denial of service attacks against the websites and networks of organizations supporting the proposed legislation. In addition, continuing conflict between Israel and its adversaries reveals the penetration of networks and the release of sensitive private data. [18] [19] Less common, but potentially more, serious are reports of attacks against SCADA systems. Recent reports of attacks against Iranian systems used to develop nuclear technologies and to enrich uranium reveal that even isolated SCADA systems are vulnerable to attack and disruption. [9] A survey of threats reveals constant attack against the world's critical infrastructure. [12]

Although the reports of constant attacks against networks and critical infrastructure create significant concerns in regards to operating in cyberspace, the benefits of operating in cyberspace has revolutionized the world. Whether thinking about the internet, cell phone systems, medical diagnostic equipment or the increased efficiencies gained through the use of SCADA systems society takes the benefits of cyberspace for granted. Fortunately, the benefits of operating in cyberspace also drive significant efforts to secure cyberspace and to prevent the disruption of networks and system operating in cyberspace. [20]

The efforts to secure cyberspace and to mitigate known vulnerabilities motivates the implementation of new technologies that prevent, detect, mitigate, and repair the damage from attacks in cyberspace. Even as malicious actors move to infiltrate and disrupt systems in cyberspace, several factors work to prevent attacks and to mitigate effects. [21] The factors that prevent unconstrained attacks in cyberspace include the belief that the actors with the resources to perform highly destructive attacks are rational. As rational actors, the cost versus benefit analysis of unconstrained cyber-attacks prevent rational actors from performing unconstrained attacks except when committing an act of war. Non-rational actors may not consider the cost versus benefit, but the non-rational actors are believed to lack the resources and discipline to coordinate and execute the most damaging levels of attack. [20]

Just as many analysts believe the most damaging cyber-attacks are constrained by rationality or lack of resources, cyber-defense also prevents and mitigates cyber-attacks. Careful risk analysis identifies specific threats and vulnerabilities and cyber-defense actions match mechanisms or policies required to mitigate vulnerabilities. By applying cyber-defense actions and practices, the adversary must expend greater resources and increase risk detection in order to penetrate or disrupt networks and computer systems. [20] [21] [22]

This research evaluates a system attempting to mitigate the effects of a cyber-attack while responding to a relatively rare power disturbance. The research relies on the assumption of appropriate cyber-defenses as well as the assumption of a rational actor not elevating the cyber-attack to resemble an act of war, or a non-rational actor with resource constraints. Given these assumptions, introducing limitations to the adversary's capabilities supports the development of distributed decision making communication enabled SPS that utilizes trust mechanisms and enables the application of game theory principles to successfully operate in a hostile, compromised network environment.

2.2 SCADA System Overview

At the most basic level, SCADA systems are simply process control systems and SCADA is often used generically to refer to a wide range of process systems. [23] SCADA systems control a variety of commercial and industrial processes ranging from processes contained in a single facility to distributed interconnected systems spanning a large geographic area. [1] When focusing in a more detailed manner, SCADA systems share several design attributes, or basic building blocks. First, almost every SCADA system has a Human Machine Interface (HMI). From this HMI, a human controller can view many aspects of the system's parameters and influence the operation of the system through the Master Control Unit (MCU). The MCU is the focal point for SCADA system. The MCU collects the data from end points in the system, and uses system logic to issue commands to control the process being monitored. Distributed throughout the system, Remote Terminal Units (RTUs) represent the end points of the system. A variety of capabilities exist in RTUs. The most basic RTUs acquire and forward sensor data to the MCU and receive commands from the MCU to control devices with little to no local logic or autonomous decision making. More advanced RTUs or Intelligent Electronic Devices (IEDs) include additional logic and processing capability. The more advanced IEDs perform monitoring tasks and local process control autonomously while reporting telemetry to the MCU and executing commands from the MCU [24] [4] [25]. In addition to the basic building blocks, SCADA systems often have other subsystems that include history servers, field control units, remote operator workstations and several other types of system and process management or middleware devices. [4] [25]

Understanding the development of SCADA systems helps illustrate many of the strengths and limitations found in traditional SCADA systems. Additionally, this understanding helps demonstrate challenges to merging SCADA system into modern IT communication systems. Some of the earliest examples of a system resembling a modern SCADA system developed as part of the power industry in the 1930s. In these earliest systems, the system controlled end devices, such as switches and breakers, used analog signals over voice circuits. Industries developed the first digital SCADA systems in the 1960s. The realities in the state of technology during the 1960s influenced many of the design decisions that continue to influence SCADA systems today. As utilities developed SCADA systems, the utilities focused on reliability as a primary design consideration. This design consideration resulted in expensive, highly reliable components with long life spans. [4] This long life span resulted in SCADA system components reliably operating 15-25 years. [4] [26]

Additionally, the initial development of SCADA system in the 1960s occurred when very few of the current IT systems existed. The resulting design of early SCADA systems relied on independent, self-contained, special purpose communications systems. In this environment, developers assumed deterministic communications mediums rather than the “best effort” models provided in most modern IT systems. [4] [3] Early designers focused almost exclusively on physical security, with little concept of network security. [23] As IT systems developed, IT systems offered reduced cost and increased capabilities over the expensive dedicated communication networks found in early SCADA systems. SCADA designs began to take advantage of the new IT technologies without adequate collaboration between IT and SCADA system designers and implementers. [4]

2.2.1 SCADA vs. Traditional IT

The lack of adequate collaboration between SCADA system designers and implementers resulted in an increase in risks and vulnerabilities for the processes supervised by the SCADA systems. The design consideration did not adequately consider communication performance requirements, network security risks and vulnerabilities of each technology, nor the many implications of the melding of the two capabilities. [4] At the center of the problem, IT communication mediums failed to provide the assumed level of security or guarantee the required level of performance required for the SCADA systems. Even SCADA systems relying primarily on dedicated communication mediums experience significant increase in vulnerabilities from connections of IT systems for business or management functions. [27]. The lack of adequate compatibility between IT and SCADA system designs creates a need for considerable improvements in the merging of SCADA and IT communication systems. Additionally, federal regulations, policies and executive orders create the requirement for improvement in SCADA systems involved in controlling critical infrastructure. [25] Table 2 compares and contrasts many of the design considerations that complicate the melding of traditional SCADA and IT systems together. [4] Table 3 illustrates several SCADA and Power Grid communication response time requirements. The delays specified in Table 3 include the time required to observe and make a decision whether to take an action, as well as the time to communicate the decision to the appropriate device to take the action. [28]

Table 2. Comparison of IT and SCADA Design Considerations [4]

Attribute	IT	SCADA
Confidentiality Requirements	High	Low
Integrity Requirements	Low to Moderate	Very High
Availability Requirements	Low to Moderate	Very High
Authentication Requirements	Moderate	High
Time Criticality	Delay Tolerant	Critical
Patching/Update	Frequent	Slow or Impossible
System Life Cycle	3-5 Years	15-125 Years
Software Changes	Frequent, Formal and Documented	Rare, Informal, Not Always Documented
Interoperability	Not Critical	Critical, Often With No Security Considerations
Computing Resources	"Unlimited" with Upgrades	Limited to Older Microprocessors
Bandwidth Available	High	Limited
Security Testing	Full Penetration Testing	Limited Penetration Testing of Human Interface. No Penetration Test of Field Devices
Operating Systems	Cots	Cots and Custom Embedded
Impacts of Security Compromise	Business Impacts	Business and Physical Impacts

Table 3. Example of Typical SCADA and Power Transmission System Communication Requirements [28]

System	Situation	Response Time
Substation IEDs, Primary short circuit protection and control	Routine power equipment signal measurement	Every 2-4 ms
	Local-area disturbance [5]	<4ms from event detection to sending notification [29]
		4-40 ms automatic response time
Backup protection and control; Wide area protection and control (WaPaC) (i.e. SPS)	Transient voltage instability	Often ≤ 180ms to convey 14+ trip signals to disconnect generators at the top generating station [30]
	Frequency instability, must respond faster than generator governors to trip generators instantaneously	Could require < 300ms response time (by load shedding) for high rates of frequency decay; requires detection within 100ms to allow operator response in 150 to 300ms [30]
	Dynamic instability	A few seconds
	Poorly damped or un-damped oscillations	Several seconds
	Voltage instability	Up to a few minutes
	Thermal overload	Several minutes for severe overloads, rarely less than a few seconds for minor occurrences [30]
SCADA	Emergency event notification	<6 ms
	Routine transactions	< 540 ms [31]
	Routine HMI status polling from substation field devices	Every 2 seconds

2.3 Smart Grid Concepts

The smart grid is the future evolution of traditional SCADA systems controlling the national power grid using network enabled SCADA systems and protocols. While a number of smart grid initiatives have begun, the realization of the smart grid remains in the future and defining all of the specifics of the smart grid remains elusive. However, one of the foci of smart grid evolution is a move from a centralized, producer controlled network to a less centralized and more consumer friendly, interactive network for producing, transmitting and distributing power. [32] Some of the goals for the smart grid include: consumer participation, accommodation of all power generation and storage options, enabling new products, markets and services, providing power quality for a range of needs, optimizing asset utilization and operational efficiency, improving operational resiliency to disturbances, attacks and disasters, relieving transmission bottlenecks, enabling self-healing and increasing system capacity. [32] [33]

Several factors complicate the evolution of the smart-grid. First, transmission systems were not originally master planned. The power grid began as a patchwork of independent utilities established to meet local requirements. [34] Much of the effort to carefully plan and engineer interconnections between power grids primarily facilitates power sales, and does not necessarily focus on preventing or improving stability or reliability through disturbances. [34] Second, the ratio of publically owned and privately owned transmission systems varies from region to region, with 60-80% of transmission systems being privately owned. [34] Third, the nation's regulatory framework provides multiple layers of rules with sometimes divergent goals. The regulations attempt to achieve a balance between reliability, availability and other often incompatible interests. [34]

Although several different visions for the development of the smart grid exist, there are many common functions. The first common function is transmission monitoring and reliability. Improvements to transmission monitoring and reliability include systems to provide real-time monitoring of grid conditions, improved automation and diagnosis of grid disturbances, and better feedback for the operators who must respond to disturbances. Additionally, automated responses to grid failures are an integral part of improving transmission monitoring and reliability. The automated systems isolate disturbed zones and prevent or limit cascading blackouts that can spread over a wide area. Many of the transmission monitoring and reliability initiatives develop the idea of “self-healing”. [35] Finally, improvements to transmission monitoring and reliability also include the idea of “plug and play” capability. The “plug and play” capability would allow for the connection of new generation plants and sources without lengthy, time consuming interconnection studies or physical upgrades to the transmission system. [34]

A second common function of the smart grid focuses on consumer energy management. The development of consumer energy management should include several capabilities. Consumers of power should have the ability to shift energy usage patterns to avoid periods of expensive peak demand resulting in lower energy costs. Additionally, utilities should have the ability to reduce a customer’s consumption when systems conditions require reduced power usage. [35] Consumer energy management systems should also include the capability to detect transmission line and equipment failures and isolate failures to prevent blackouts from spreading. Early examples of consumer energy management successfully demonstrated the reduction of significant portions of peak demand through consumer actions rather than increasing power output. [34]

2.3.1 Special Protection Systems

Among the many objectives and goals for the smart grid, this research focuses on a system that automates responses to grid failures, isolates disturbed zones and prevents or limits cascading blackouts that can spread over a wide area. This is a Special Protection System (SPS). A traditional Special Protection System monitors key generation assets, transmission lines and their associated flows in near real-time. [36] [37] When a change of status is detected, a pre-programmed set of actions takes place. These actions include opening one or more power lines, High Voltage Direct Current power Transfers, (HVDC), wide area load shedding, generator re-dispatch and generator rejection. [36] Table 4 lists the most commonly used SPS types with generator rejection, load rejection and underfrequency load shedding being the most common. Future versions of these systems may also allow for power transfers beyond normal limits and allow transmission lines to operate closer to thermal limits and beyond normal system voltage or stability limits. [38].

Table 4. Percentages of Most Common SPS Types [36]

Type of SPS	**Percentage**
Generator Rejection	21.6
Load Rejection	10.8
Underfrequency Load Shedding	8.2
System Separation	6.3
Turbine Valve Control	6.3
Load & Generator Rejection	4.5
Stabilizers	4.5
HVDC Controls	3.6
Out-of-Step Relaying	2.7
Discrete Excitation Control	1.8
Dynamic Braking	1.8
Generator Runback	1.8
VAR Compensation	1.8
Combination Schemes	11.7
Others	12.6

A review of the power industries' experiences with Special Protection Schemes reveals increased deployment and use of SPSs. The review also reveals significant expenses related to the failure of SPSs to perform their functions and the unnecessary operation of SPSs. Additionally, approximately 35% of responding power operators reported no reliability models or computational models to validate the SPSs design. Finally, the study reveals concerns about the performance of load rejection schemes compared to other SPS schemes. [36]

One possible approach to implementing many aspects of the smart grid is to utilize Distributed Intelligent Agent based systems. [38] In this vision for the smart grid, Distributed Intelligent Agents provide decentralized monitoring and control of smart grid functions. A distributed agent based SPS is one of the foci of this research.

Better understanding of the role of SPSs requires a brief introduction to Power System Stability Control and the definition of terms. In *Power System Stability and Control,* Prabha Kundar broadly defines power system stability as

> *…that property of a power system that enables it to remain in a state of operating equilibrium under normal operating conditions and to regain an acceptable state of equilibrium after being subjected to a disturbance.* [39]

In normal operations, power systems experience many sizes and types of disturbances. Load changes, equipment malfunction, weather, natural disasters, and potentially cyber-attacks can cause power system disturbances. The properties of the system and the functionality of special protective devices influence a systems ability to maintain or regain stability after a disturbance. [39] Normal system stability disruptions include rotor angle and voltage stability. These are generally short-term stability events. [39] Typically, regular system regulation and control functions automatically maintain system stability during these types of disturbances.

In addition to dealing with disturbances within system design specification, severe upsets also effect power systems. The larger upsets produce effects beyond the ability of systems to automatically correct and require a higher level approach to maintain or regaining stability. This higher level response can result in "islanding" or isolating parts of the power system. "Stability in this case is a question of whether or not each island will reach an acceptable state of operating equilibrium with minimal loss of load" [39] These severe disturbances are the types of disturbances that require SPSs. The severe disturbances and the SPS responses are analyzed with mid to long-term simulations.

The simulation analyzed in this research involves a severe system disturbance that requires a higher level response, or an SPS response, in order to maintain system stability. Specifically, a transmission line failure creates a power flow disturbance that requires the rejection of a group of generators. The rejection of the generators creates two islands in the power grid and results in an imbalance between the generator capacity and the load requirements of the power grid. The imbalance between generator capacity and the load produces a dangerous frequency drop. The SPS must analyze its observation of the power grid and determine the appropriate actions required to regain system stability. The SPS action prevents the conditions that could otherwise result in large scale cascading blackouts in the power grid.

Understanding why the SPS must respond in this scenario requires additional background knowledge of power system design. Turbines used for power production are designed to operate at a specific frequency and are damaged when operating at higher or lower frequencies. The increase in stress related damage from a deviation in frequency significantly reduces the operational life span of the turbines. Additionally, periods of high stress are cumulative; a few minutes of underfrequency can reduce the turbines' operational life span by years. [39] Periods of underfrequency operation pose a critical problem since power output cannot be increased to more than the generator's design capacity. [39] Additionally, limits to how quickly a turbine can increase its output exist. Typically, generators can increase output quickly by about 10%. After the initial increase in generator output the generator can only increase output by about 2% per minute, and then, only up to the maximum design output. [39] To protect the turbines from damage, underfrequency relays typically trip if a generator falls below 57.5 Hz for more than 10 seconds or trip instantly if the frequency drops below 56.0 Hz. In order to prevent a generator from tripping off on underfrequency relays or from operating at lower than normal frequencies for extended periods, SPSs employ load shedding schemes to reduce the loads on the generators. Figure 1 illustrates the typical operating frequency limitations for steam turbines.

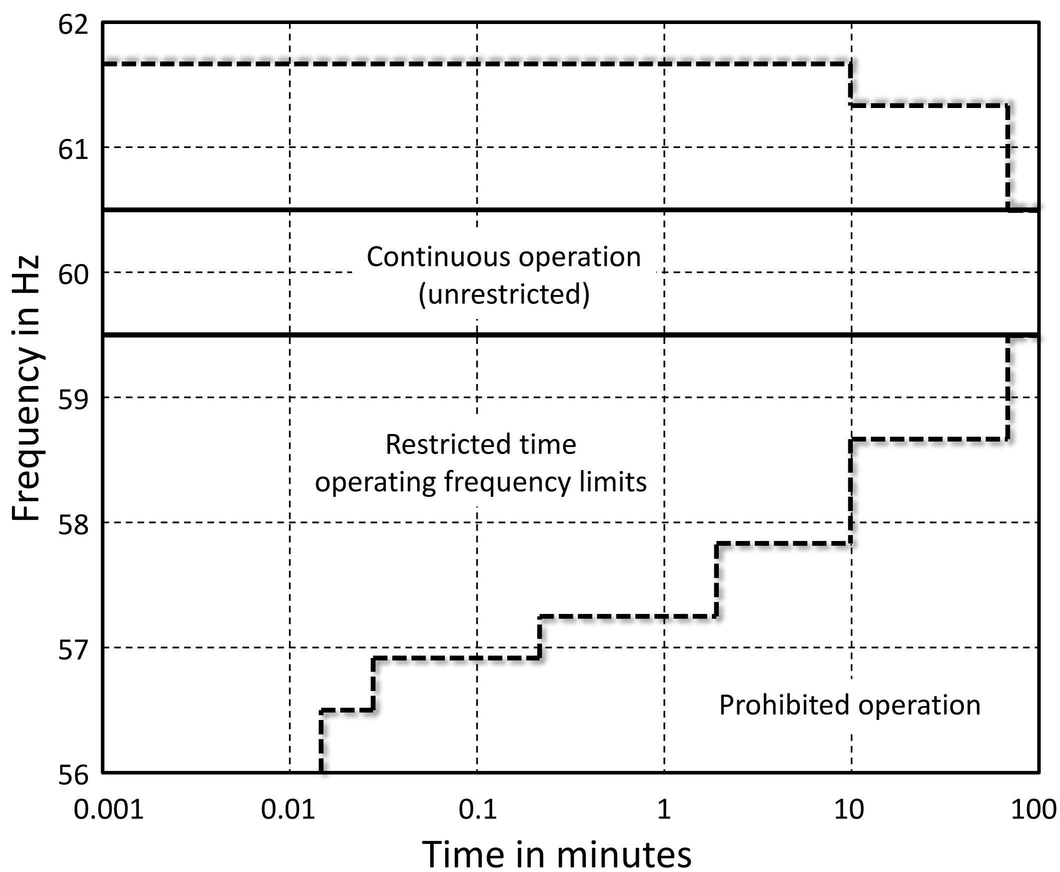

Figure 1. Steam Turbine Partial or Full Load Operating Limitations During Abnormal Frequency, Representing Composite Worst-Case Limitations of Five Manufacturers [40]

Traditional load shedding schemes consist of dropping predetermined amounts of load. A typical load shedding strategy consists of dropping 10% load at 59.2 Hz, 15% load at 58.5 Hz, and 20 % load at 58 Hz. Strategies for shedding larger amounts of load consider the rate of frequency drop in addition to the frequency. [41] Typically, load shedding relays requires approximately 0.1-0.2 seconds to operate. [42] Often, the predetermined SPS load shedding may not result in an optimal solution for the current conditions. As the smart grid continues to develop, communication enabled SPSs make more intelligent shedding strategies possible. This research evaluates a system that dynamically selects an optimized load shedding strategy.

2.4 Concepts of Trust Systems

SCADA systems and concepts, like the smart grid, provide the mechanism for cost effective process control and opportunities for more efficient operation of industrial processes and utility systems. As discussed previously, SCADA systems evolved without network security as a priority. This lack of network security resulted in the creation and exposure of significant vulnerabilities and opened critical processes and systems to serious external threats. As awareness of the seriousness of the threat and the degree of the risk increased, cyber professionals and government regulators began pushing for increased security in SCADA systems. [4] This push for improved security for SCADA systems, specifically those systems controlling the nation’s critical infrastructure, resulted in the establishment of regulations and a focus on SCADA security related research. [25] [3] Many of the regulations and much of the research focused on applying and adapting traditional network security mechanisms and policies for network enabled SCADA systems. The traditional network security mechanisms include firewalls, Intrusion Detection Systems (IDS), encryption techniques, logical network provisioning and enforcement of policies and protocols. [3] While the adaptation of existing network security mechanisms provides a starting point for securing SCADA system, these approaches have limitations. The existing security mechanisms fail to address many of the unique operational requirements or security vulnerabilities present in SCADA systems. [4] [3] [43] This failure of traditional security mechanisms drives alternative research efforts that include the development of specialized trust systems.

2.4.1 Trust in Computer Systems and Networks

The concept of the smart grid utilizing agent based processes introduces the possibility of peer-to-peer networks between intelligent agents. Dr. Stephen Marsh worked to formalize concepts of trust to deal with multi-agent systems. In [44] Dr. Stephen Marsh presents several concepts of trust. The effort to define trust revealed common concepts in the formulation of trust. The central defining concept was that trust deals with levels of confidence in the face of uncertainty. This level of confidence describes how strongly an agent believes another agent will perform a desired function.

In traditional computer and networking systems, trust is often granted by design between dependent processes or through simple policy or protocol enforcement mechanisms. Typically, the systems make trust decisions using unchanging criteria without consideration of behavioral changes over time or assessment of what is done with the trust granted. Traditional network and computer systems rely on policy or protocol trust mechanisms which enforce rules, but not necessarily behaviors. In networks, messages conforming to the protocol standards are generally trusted. In computer systems, the proper credentials grant access to all the privileges granted to the holder of the credentials. Traditional network and computer systems have no mechanisms for assessing or adapting to past performance, to detect changes in the trustworthiness of sources and destinations or to determine the trustworthiness of the data being sent. [45] [46]

Compared to traditional network and computer trust mechanisms, trust is a more critical aspect of nearly every interaction in distributed systems. Distributed agent based systems typically make decisions based on the inputs received from other independent agents, rather than dependent processes. This high reliance on the inputs from other independent agents makes trust in distributed systems a more fundamental aspect of system design. [47]

In [47], the authors define trust in multi-agent systems as, “Trust is a belief an agent has that the other party will do what it says it will…” The authors continue by breaking multi-agent trust into two complimentary levels: individual level trust and system level trust. System level trust is the trust gained by the enforcement of rules (i.e protocols and mechanisms). The individual level of trust is based on the beliefs held about the other individual agents in the system based on direct and indirect observations of the other agent’s actions. A goal of individual trust and system level trust is to balance efficiency with the need for manageable levels of uncertainty. This research focuses on the individual level of trust rather than trust based on enforcement of policy or protocol.

Systems generally establish trust through a variety of mechanisms including policy, location, bio-metrics, reputation or a combination of these factors. [48] Each factor can provide information required to establish trust at both the system and individual levels. Often trust systems evaluate the factors subjectively with the expectation of changing levels of trust. The subjective nature of the evaluations result in the assumption that past actions do not necessarily represent future performance; other factors may also contribute to establishing trust. The amount of historic data required varies for different systems and applications. [45]

2.4.2 Trust Models

At the individual trust level, several basic trust models exist. The basic trust models include learning and evolution based models, reputation based models and socio-cognitive based models. Learning and evolutionary models assume multiple interactions between agents. The learning models also assume that some benefit arises for an agent defecting, or not performing as expected, but the defecting agent experiences a loss in possible future benefit from the defection. The loss of possible future benefit defines the concept of regret in a learning trust model. [47]

Reputation trust models focuses on beliefs about an agent created by both direct and indirect observations. Reputation based trust systems often aggregate the direct and indirect observations. Reputation models evaluate an agent’s past behavior to predict likely future behavior in order to establish trust. [45] [47] [49] Socio-cognitive models of trust produce determination of trust based on more subjective assessments of other agents. The assessment includes belief about another agent's competence, willingness, persistence and motivation. [47] [45]

2.4.3 Trust Applied to an SPS

In addition to the general concepts of trust, this research builds from previous research efforts found in [50] [51] [52]. In Jose Fadul's PhD dissertation, he demonstrated an SPS utilizing simple reputation based trust between communication enabled agents could successfully perform SPS functions. Specifically, the system could operate in an environment with detectable malfunctions or malicious nodes. Using concepts of reputation based trust Fadul's SPS decision making agent detected malfunctioning or malicious nodes and devised an SPS strategy that avoided using untrusted nodes. This research refines Fadul's simple reputation based trust to operate in environments with packet loss and delay by assessing trust based on trends observed in past and present interactions between nodes. In addition to the reputation based trust mechanisms, the agents in this research also utilize aspects of cognitive based trust.

Past research assumed malfunctions or malicious actions were detectable. This research assumes malfunction and malicious actions are only detectable with a 90% probability. The cognitive aspect of the trust deals with an assessment of the competence and the persistence of the agents in the SPS. The assessment of competence and persistence results in an SPS strategy that spreads the risk of undetected malfunctions across enough agents that successful SPS actions become highly probable (98% or greater).

2.5 Game Theory Fundamentals

When evaluating the study of cyber security concerned with IT and SCADA systems, significant research continues to focus on policy formulation and enforcement, management practices and with improving the security of the lower levels of the TCP/IP network model. Much of this research evaluates existing IT and SCADA technologies with the understanding that the longevity of SCADA system components requires adaptation, protection and securing of older systems and protocols designed with few if any security considerations and with limited hardware capability. [4] [25] However, the concepts guiding the deployment of the smart grid enables research into systems built around projected network and SCADA capabilities. [53] These future capabilities envision Intelligent Electronic Devises (IEDs) capable of increased functionality as independent agents. Additionally, this increase in future capability utilizing independent agents enables alternative approaches to formulate optimization, security and protection problems into a strategic game, and then for the application of game theory principles.

2.5.1 Game Theory Foundation

Although participants probably had no concept of game theory, a brief investigation into the history of game theory suggests that game theoretic principles were applied as long ago as 0-500AD. The Babylonian Talmud appears to utilize a cooperative game theoretic approach for the division of wealth to widows upon the death of their husband. [14] In the Early 18th century, James Waldergrave developed the first known example of the min-max mixed strategy for a two-person game. [54] In large part, game theory continued to develop as research in economic and social sciences applied mathematical rigor to describe and model observed behaviors. The primary formulations for modern game theory developed in the early to mid-1900's. During this period John von Neumann published a proof for the min-max theorem and John Nash established the existence of the "Nash Equilibrium" concept. John Nash and John von Neumann, along with several others, formally developed the current ideas that define game theory. [54] While game theory developed to address economics, refinement of game theory outside of economics continues to grow.

The first step in introducing the present state of game theory is to establish a working definition. Game theory is a set of theories, principles and tools that provide a systematic method for modeling strategic situations (games), in which an individual's success in making choices depends on the choices of others. [14] [54] [48] Game theory can model a variety of strategic relationships from 2 players to n-players. The players can be human or can be other agents. A fundamental premise of game theory is the idea of utility or cost functions that define the benefits received or the amount of cost associated with each strategy. [14]

One of the first principles of game theory is the idea of cooperative vs. non-cooperative vs. hybrid game. In a cooperative game, players achieve the highest levels of utility or lowest cost when cooperative. [55] A cooperative game also implies mechanisms to enforce cooperation in coalition members and communication between coalition members. [56] Non-Cooperative games do not include external mechanisms to enforce strategy and assume each player makes decisions independent from other players. Non-cooperative games must be self-enforcing. [57] Hybrid games include some communication capability, but have no mechanisms to enforce a strategy. The approach used in this research most resembles a hybrid game. Each SPS agent is a member of a coalition. Communication is assumed between members of the coalition; however, no external mechanism enforces a strategy. The design of the game views the adversary as a single agent. However, the adversary could be designed as a multi-agent coalition as well.

A second principle for defining the characteristics of a game is whether a game is simultaneous or dynamic. In a simultaneous game, all players determine their course of action and perform their actions at the same time, or without any knowledge of actions selected by the other players. [56] [48] A dynamic game occurs over time. In a dynamic game, players have multiple turns to take actions. In a dynamic game, players typically select actions with knowledge of the past actions selected by other players. [48] The approach used in this research results in a simultaneous game where the SPS players determine a strategy for defending the system and the adversary determines a strategy for attacking the system.

A third principle of defining the characteristic of a game is the idea of symmetric vs. asymmetric game. In a symmetric game, each player has the same strategies available and the cost or payoff depends only on the strategy selected, not on the player selecting the strategy. An asymmetric game consists of players who have different possible strategies, or players who receive different benefits or costs for the same strategies. Therefore, the benefit received depends on player not just the strategy. [56] The approach used in this research forms an asymmetric game.

Another characteristic of a game is the degree of knowledge each player has about the other players and about the game state. The amount of knowledge can vary from complete, perfect, imperfect and incomplete knowledge. Complete information implies each player knows the strategies and the utilities available for all players in the game. [57] However, this does not imply knowledge of actions selected by players in the past. Perfect knowledge implies that all of the actions taken by other players in the past is known, but does not imply knowledge of all strategies or utilities available to other players. A perfect game implies a sequential or dynamic game. [14] Imperfect game implies at least some of the other player's actions are not observable. An incomplete game implies that players are not fully aware of the strategies or utilities available to all of the players. Bayesian games are incomplete games. Players use probabilities formed from limited observations and beliefs to select the action in an incomplete game. [56] The game formulation in this research is an incomplete game.

The concept of zero-sum games vs. non-zero sum games is another characteristic of game theory. In a zero-sum game, the total benefit achieved by all players in game sums to zero or some other constant. The constant sum property of zero-sum games results in definite winners, losers or ties among players. A non-zero-sum game does not require total utility to sum to zero. In a non-zero sum game, all players can achieve positive or negative utility. As a result, a non-zero-sum game can model a greater range of strategic relationships. [57] [58] This research uses a non-zero-sum game.

Similar to dynamic vs. simultaneous games is the concept of single vs. repeated games. A single game is a game played only one time. The players have only one opportunity to select a strategy. A repeated game is similar to a dynamic game except the same game is repeated multiple times rather than taking turns in a single game with different states determined by past player actions. [14] In a repeated game, players can choose a different strategy after each round of play. Depending on the formulation of the utility function, the best strategy for a repeated game can vary significantly from the best strategy for a one-time simultaneous game. [56] This research utilizes a single game.

Dominant strategies are another important characteristic of games. Dominate strategy concepts are important when analyzing a game model. A strictly dominate strategy is a strategy that always provides a player with better results regardless of the other player's strategy. The opposite is a strictly dominated strategy which is never the best strategy. [48] A weakly dominate strategy provides equal or better results, where a weakly dominated strategy provides equal or worse results. The game formulation in this research provides for both strictly and weakly dominate/dominated strategies depending the goals that determine the utility function.

Related to dominate/dominated strategies are the ideas of Nash Equilibriums and Pareto Optimal strategy. The Nash Equilibrium concept provides an important game theory principle. The Nash Equilibrium point is a best strategy given the other players possible strategies. In a Nash Equilibrium, no player has an incentive to unilaterally change strategies. A Pareto Optimal strategy is the point where the players have the maximum utility. Failure to guarantee a Pareto Optimal strategy is a significant limitation of the Nash Equilibrium. A non Pareto Optimal Nash Equilibrium results when all players could benefit more if the all players changed strategy, but not by unilateral strategy changes. Within the Nash Equilibrium there is also the concept of pure and mixed strategy equilibriums. Pure Nash Equilibrium results when a strategy is always the best given the adversary's strategies. Mixed Nash Equilibriums result from a probability distribution over possible strategies that produces the best results given the adversary's possible strategies. [14] Technically, a pure Nash Equilibrium is a type of mixed strategy Nash Equilibrium. [54] Nash also demonstrated that at least one mixed strategy equilibrium exists for any game with a finite set of actions. [14]

2.6 Previous Research

Several approaches to improving the agent based SPS contributed to the development of the SPS agents utilized in this research. Initial development of the federated power system and network simulator utilized a simple SPS agent that demonstrated the viability of the simulation environment and of the scenario to test SPS actions. In this initial research effort, the SPS relied on a single SPS control agent to monitor all of the system parameters observed from the inputs received by the generator and load agents and to determine the SPS strategy. The initial research demonstrated the SPS's ability to perform SPS actions and to maintain system stability when faced with up to 5% communication loss. [51] [50]

Additional research using the simulation environment and SPS scenario added a more realistic model of typical network traffic observed in a SCADA network shared with a limited amount of IT network traffic. The research evaluated strategies to maintain reliable SPS actions while experiencing delay and communication loss due to network congestion. The research evaluated the use of bandwidth reservation mechanisms and the use of Exponential Weighted Moving Average to prevent or to compensate for communication loss due to network congestion. [59] This research also relied on a single SPS control agent to monitor the power grid and determine the SPS strategy.

The next related research continued using this SPS scenario with the introduction of malicious/malfunctioning nodes and simple reputation based trust mechanisms. This research demonstrated that an SPS exposed to detectable malicious/malfunctioning nodes could use a majority rules reputation based trust mechanism to detect bad nodes and develop successful SPS strategies. This research removed the background traffic and focused on the ability of the system to detect bad nodes and then to exclude the bad nodes from the SPS strategy. This research also relied on a single SPS control agent to monitor the power grid and determine the appropriate SPS strategy. [52]

In previous research, generator and load agents reported system observations to a centralized SPS control agent to determine levels of trust based on an analysis of the system observations. That centralized SPS agent utilized the system observations to develop system knowledge and then to determine an appropriate strategy for maintaining system stability following a disturbance. Finally, the centralized SPS agent issued commands to trusted generator and load agents to implement the strategy.

2.7 Summary

The SCADA systems that make up the nation's electric power generation and transmission systems are in the process of evolving into the smart grid. This evolution is transforming systems that experienced little significant change for decades from a centralized, producer-controlled network to one less centralized and more consumer interactive. While these changes bring new challenges and vulnerabilities, the communication enabled smart grid also brings the opportunity to strengthen the power grid's ability to respond to significant disturbances and to improve reliability. Additionally, the agent based paradigm enabled by the smart grid permits new approaches to improve security and protection of smart grid function. These new approaches include the development of trust mechanisms and use of game theory to improve the smart grid's ability to perform SPS functions when faced with malicious actions and malfunctions. Finally, previous research to develop an appropriate simulation environment and SPS scenario enables the evaluation of a several variables and mechanisms. The ability to evaluate a several variables and mechanisms allows for research to test new solutions for the challenge of securing and protecting an SPS specifically, and the smart grid, in general.

III. Methodology Stage One-Three

3.1 Chapter Overview

This research methodology explores and analyzes a proposed Special Protection System (SPS) that addresses system modernization and transmission system reliability directly and other areas of the smart grid development indirectly. Specifically, the research continues the study of applying simple trust based mechanisms to communication enabled SPSs. Previous research focused on utilizing smart grid concepts in conjunction with simple trust based mechanisms to improve the reliability, security and effectiveness of a distributed SPS with a centralized decision-making process. However, this research begins by focusing on testing and analyzing a distributed agent based SPS with a distributed decision-making process utilizing smart grid concepts and simple reputation based trust mechanisms to improve the reliability, security and effectiveness of a communication enabled SPS. Next, the research continues by evaluating the distributed SPS's decision-making process performance when coping with communication delays and loss caused by background traffic and communication malfunctions and/or malicious actions. The research continues testing the distributed SPS's performance against a fully detectable adversary attempting to disrupt the SPS's actions while experiencing delays and loss caused by background traffic and communication malfunctions or malicious actions. In the first three stages of this research, the SPS had no limitations on the monitoring of system agents as part of the security strategy.

The decentralized decision making communication enabled SPS is a significant departure from traditional SPSs and recently explored centralized decision making communication enabled SPSs. By reducing the vulnerability inherent in the single point of failure found in centralized SPSs, this decentralized system provides the potential for increased reliability and security.

3.2 Problem Definition

3.2.1 Goals and Hypothesis

There are several stages in the performance of this research methodology. In each stage specific goals exist to answer a hypothesis. Hypothesis for Stage One:

A distributed decision making communication enabled SPS using simple reputation based trust can successfully determine and execute an appropriate SPS load shedding strategy while experiencing various levels of disrupted agents.

During the first stage of the research, the primary goal is to test a distributed decision making communication enabled SPS to determine a level of success and to compare the performance to centralized decision making communication enabled SPSs used in past research. In the first stage of the research the distributed SPS agents use a trust mechanism and an SPS load shedding strategy similar to mechanisms and strategies used in past research. [52] The first stage tests the SPS with background traffic but not with network delays and losses caused by malicious actions. This stage of the research seeks to determine whether this model of a distributed decision making SPS successfully determines and executes a successful load shedding strategy with detectable disrupted or malfunctioning generator and load agents.

Hypothesis Stage Two:

A distributed decision making communication enabled SPS using simple reputation based trust can successfully determine and execute an appropriate SPS load shedding strategy while experiencing various levels of network traffic and losses.

During the second stage of the research, the primary goal is to evaluate the performance of a modified distributed decision making SPS when operating on a network with background traffic and communication delays and losses caused by malfunctions and adversarial disruptions without attacks against the system nodes. The SPS agents in this stage of the research are modified to include a retransmission mechanism to overcome the low to moderate amounts of communication loss. This stage of the research seeks to determine whether the mechanism to overcome communication loss allows the distributed decision making SPS to successfully determine and execute a successful SPS load shedding strategy while dealing with low to moderate communication delays and losses.

Hypothesis Stage Three:

A distributed decision making communication enabled SPS using simple reputation based trust can successfully determine and execute an appropriate SPS load shedding strategy while experiencing various levels of network traffic and losses and various levels of disrupted agents.

The primary goal for the third stage of the research is to test the performance of a modified distributed decision making communication enabled SPS when operating on a communication network with background traffic, communication delays and losses caused by malfunctions or adversarial disruptions and with disruption or malfunction of generator and load agents. The SPS agents in this stage of the research include a mechanism to overcome communication loss as well as a mechanism to determine levels of trust for other agents in the system. In this stage, the research seeks to determine whether the mechanism to overcome communication loss as well as the mechanism to determine trust work together to allow the modified distributed decision making to determine and execute a successful load shedding strategy while operating with communication delays and losses, and with detectable disrupted or malfunctioning generator and load agents.

A minimum level of success for the SPS is defined by the SPS detecting the system disturbance and then maintaining system stability by shedding load quickly and accurately enough to prevent the system frequency from dropping below the critical level. Increased success results from minimizing the cost of the SPS strategy. The cost is minimized by shedding the minimum amount of load required to maintain the system frequency above the critical level. Additionally, the degree of success is measured by comparing the distributed SPS agent’s performance to traditional SPSs and the expected performance of network enabled SPSs from previous research.

Testing these research hypotheses drives significant changes from the basic operation of traditional SPSs. A traditional SPS does not utilize an adaptive approach to maintain system stability. Traditional SPSs protect system components from damage and can prevent large scale blackouts under predetermined scenarios. The pre-coordinated strategy does not result in any optimization of the protective actions. The traditional SPS's lack of dynamic strategy often results in sub-optimal capacity shedding. [37] This sub-optimal shedding results in the rejection of more load than required, increasing cost or results in the rejection of less load than required, increasing the probability of widespread uncontrolled blackouts. A traditional SPS also fails to consider other factors such as trustworthiness of system components. Rather than a script to deal with predicted disturbances, a communication enabled SPS reacts dynamically to the system state while considering many factors not considered by a traditional SPS.

In addition to changes from traditional SPSs, the research hypothesis also drives changes from the operation of recently researched centralized communication enabled SPSs. Past research evaluated the performance of a centralized communication enabled SPS with background traffic related delays or with trust mechanisms to detect untrustworthy load and generator agents. The past research efforts did not combine both challenges at the same time. [59] [51] [52] Past research into a communication enabled SPS with background traffic did not evaluate minimization of costs related to excess load shedding. [59] Additionally, the previous research using an SPS with background traffic used bandwidth reservations and estimation schemes to prevent data loss and delay or to mitigate the effects of missing data to overcome communication delays and losses. The past research with a centralized decision making SPS using a trust mechanism to detect untrustworthy agents assumed all untrustworthy agents could be detected and that the trust mechanism could be used to monitor all of the generator and load nodes. [52] Compared to the previously researched centralized SPSs, the distributed SPS requires additional network capacity for new mechanisms to overcome communication related delays and losses and should require revised trust mechanisms to deal with the communication delays and losses.

Although there are some advantages to the traditional SPS in terms of network capacity and communication equipment costs, the distributed SPS should have the advantage over both traditional and the centralized SPS in terms of reliability and security. As discussed above, a traditional SPS does not rely on any active coordination/adaptation to operate. This lack of coordinated adaptation results in almost no network or communication security vulnerabilities in determination of an SPS strategy. However, the lack of coordination also reduces the reliability of the traditional SPS by reducing the number of scenarios from which an SPS can successfully recover. Additionally, the lack of coordination prevents the detection of untrustworthy nodes, resulting in the possibility that nodes fail to execute SPS commands and the SPS fails to maintain system stability. The reliance on predetermined actions to match possible disturbances increases the probability of cascading failures compared to coordinated communication enabled SPSs. [39] When comparing the distributed SPS to the centralized system, removing the centralized SPS from being a single point of failure will likely increase the reliability and security of the power transmission grid.

3.2.2 Approach

For practical reasons, power transmission systems require SPSs. System malfunctions can create unstable conditions or disturbances. When disturbances cannot be corrected with normal system processes, the system either successfully employs protection systems, including SPSs, or risks catastrophic failure. A catastrophic failure in a power transmission grid results in widespread islanding, blackouts and possible equipment damage. The 1965 and 2003 blackouts illustrate extreme examples of what happens when multiple protection systems, including SPSs, fail to successfully react to disturbances and keep the power grid stable. [60] [61]

This research utilizes a scenario that creates a realistic special protection condition and evaluates the distributed SPS's ability to return the system to stable operation. The creation of a realistic special protection condition requires extensive electric transmission grid knowledge. In this research scenario, a disturbance requiring special protection actions is created by introducing system failures and other faults. The failures and faults create a disturbance resulting in an imbalance requiring generators to be removed from service. The sudden removal of generation capacity from the power grid creates the disturbance that requires SPS load shedding actions. Based on data gleaned from past large scale blackouts, the conditions created produce a realistic SPS disturbance. [4]

To demonstrate acceptable response to system disturbances, the research seeks to test the system operating through a data network with a variety of operating conditions, workloads and SPS Schemes. In order to test an SPS scheme, scenarios requiring an SPS intervention must be created in the simulation. However, this research is limited to evaluating a single scenario and does not address the SPS's ability to respond to alternate special protection conditions. The danger of developing a system that performs correctly for only this one scenario is a significant limitation on this research. The research attempts to keep the distributed SPS's action general enough to respond to any SPS action that requires load shedding.

3.3 Testing Environment

The primary tasks in the first three stages of this research is the development and testing of an agent based communication enabled SPS using distributed decision making agents with reputation based trust mechanisms. The testing determines the SPS's ability to successfully maintain stability of the power grid when experiencing a significant disturbance that could result in an uncontrolled cascading blackout and while experiencing malfunctions and malicious activities.

A federation of network and power simulation provides the primary evaluation method for the testing of the distributed special protection system. In this circumstance, the selection of the simulation environment stems from rational determination and circumstance. First, much of the infrastructure to enable smart grid technologies is not in place. Even the few areas where a limited smart grid capacity exists, experimenting with operational power transmission systems introduces excessive risk and cost. When modeling a regional power transmission grid, no reliable analytic models exist for measuring the interactions between power transmission systems and the coordination enabled by smart grid technologies and data networks. The tool that enables the development and the study of this SPS is a realistic simulation environment for both the power system and the communications network. The simulation environment selected for this research is the combination of the PSS/E power simulator and the NS2 network simulator federated together by the Electric Power and Communication Synchronizing

Simulator (EPOCHS). [50] [62] Figure 2 illustrates the basic configuration EPOCHS simulation environments. [51] Inside these simulation programs, specific power transmission and network models provide a realistic and validated test environment. Using this environment also provides the opportunity to compare the results of new research with existing research efforts. [52] [51] [59]

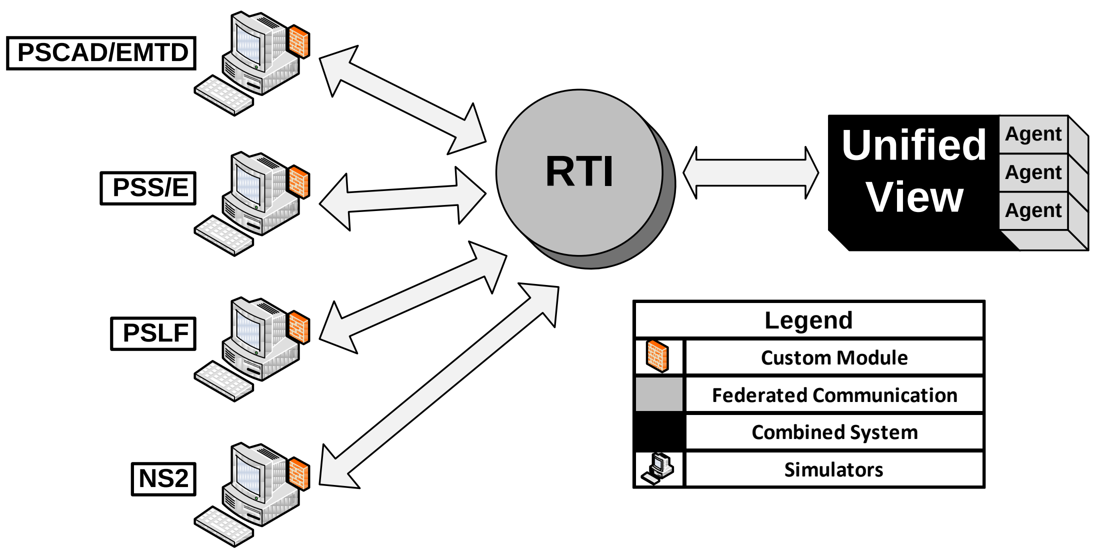

Figure 2. Graphical Representation of EPOCHS Simulation Environments [59]

Each simulation run utilizes the same basic scenario. Power transmission lines are tripped due to malfunction and overloading to create a system imbalance that requires the removal of a specific generator from the system. This results in an imbalance and creates an unstable system condition with a dropping system frequency. The distributed SPS uses the data network to determine and execute an SPS strategy to reestablish system stability by intelligently shedding load. The simulation runs for 50 seconds in the simulation environment. The factors utilized in the simulation include levels of communication loss and the location of the untrusted nodes. The research utilizes the same randomization seeds as utilized in previous research to better correlate results. An analysis of variance and a comparison of confidence intervals are used to determine the statistical significance of the simulation results. [63]

3.4 Special Protection System Test Details

The SPS test case scenario operates within system boundaries and includes the system services, the system under test, the workload the system operates under and the factors that are controlled to test and evaluate the component under test. The component under test is the SPS scheme, and each stage of the research evaluates a specific scheme's response to the testing factors. The system under test includes power transmission grid, the communications network, the load and generator nodes, the special protection nodes and the distributed special protection scheme.

3.4.1 Power Transmission Configuration

The power transmission grid provides the physical connections between generator, load nodes and other transmission system components. This research only uses one power transmission configuration. The configuration used is a modified IEEE 145-bus 50 generator test case to represent the power transmission system. [64] Modification to the original test case changes the behavior of a few generators, adds an additional power transmission line, reduces the overall generation capacity and rebalances power flows in order to increase the importance of the power flowing over key transmission lines. [51] The degree of interconnection between the nodes in the system influences the system's ability to maintain stability during disturbances. A well connected electrical grid provides more flexibility for transferring power and maintaining stability, but often contains interconnections that are not capable of transporting enough power to maintain stability during special protection situations. [39] This research models a well-connected electric transmission grid. Additional changes to the electrical transmission grid are outside the scope of this research. The IEEE test case is used in PSS/E to model transient stability during the simulated SPS actions. Figure 3 shows the logical layout of the Power Grid used in this simulation

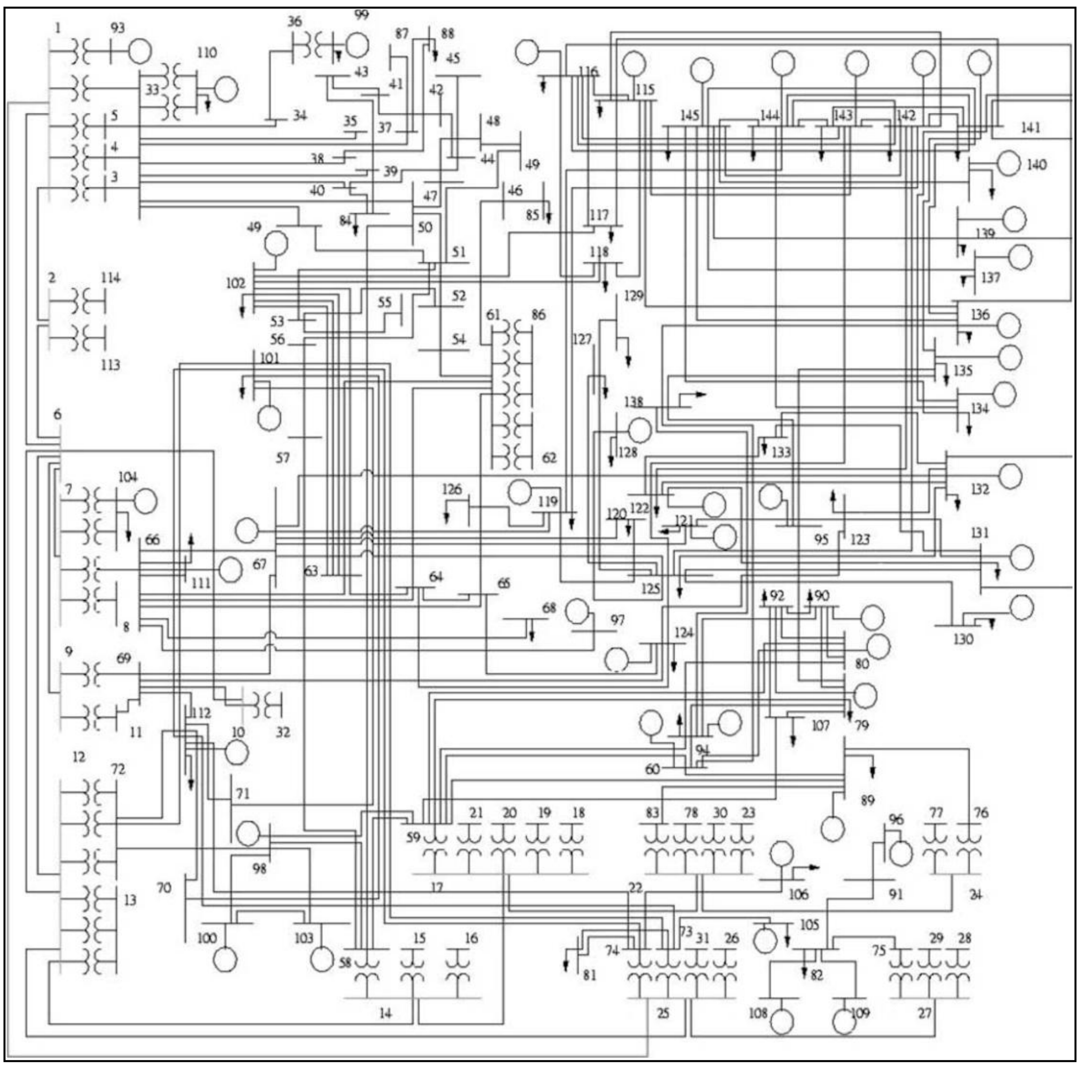

Figure 3. Logical Layout of the Power Grid [51]

The power transmission system operates at a specific workload described by the amount of power generated, the amount of power required by the loads and the amount of transmission capacity on each power transmission line. As a power transmission grid is operated closer to maximum efficiency and minimum safety levels, less reserve capacity remains. [39] In addition, larger systems have more flexibility in dealing with disturbances than a smaller system where there may be very few strategies for maintaining system stability. In a stable system, the power generated and the power required for the loads are in balance and the transmission lines are within normal operational limits. When the power generation capacity and the system load requirements do not balance, or transmission lines operate outside of normal operational limits, the system becomes unstable. Power generation and transmission systems have methods to adjust for fluctuations in power generation capacity and load requirements. A system disturbance in this research is a condition that creates an imbalance between the generation capacity, the system load and transmission line capacity too large for normal system processes to maintain stability. This simulation utilizes a power generation and load imbalance along with overloaded transmission lines to create a disturbance that requires an SPS to maintain system stability.

3.4.2 Communication Network Configuration

The communications network provides the logical connections between system nodes. The load and generator nodes utilize the communications network to share local system observations and to receive commands. The number and location of the generator and load nodes and data link capacity influences the performance of the system. This research only observes one logical communication network configuration. Additionally, the data link capacity used in this research is 100 Mbps representing the lower boundary of expected capability for future smart grid networks and is the minimum capacity required for this SPS to operate. [65] The agent based communication enabled SPS's communication network infrastructure closely mirrors the power transmission grid based on an assumption that future smart grid networks will likely run along the same routes as the power transmission systems. [37] [53] In a smart grid, the physical and logical design of the data network influences the performance and reliability of a data network. [32]

The operation of the communication network provides a workload used to test the SPS schemes. The network workload for this system includes the background network traffic, the amount of packet loss due to malicious actions or malfunctions and the number, location and detection probability of untrusted nodes in the system. The background traffic models traffic that may occur at different times in a communication network used for SCADA type traffic. The background network traffic for this research is modeled from an analysis of LAN and SCADA network traces and assumption about the utilization of future smart grid networks. [59] However, the traffic differs significantly from the traffic used in previous research with a higher probability of background traffic occurring during the critical first 300-350 ms of the simulation. Additionally, non-power related traffic is not used. Background traffic and communication losses influence the performance of the distributed SPS. Table 5 shows the background traffic utilized by this research. As background traffic and losses increase, delays in the network increase and reliability of the network decreases. [66]

Without appropriate mechanisms to overcome delays and losses, the distributed SPS can fail to meet the minimum timing requirements or fail to obtain enough data to develop an SPS. The background traffic in this simulation uses the same background traffic mechanisms used in previous research with higher occurrence rates and modified packet sizes. The traffic falls between the medium and high levels from [59].

Table 5. Background Traffic Rates [66]

Background Traffic Type	Distribution	Packet Size	Rate
SCADA	Constant	44 Bytes	One every 4ms per bus
Power Quality Data	Poisson	76-196 Bytes	One every 10ms per bus
Routine Internal Traffic	Poisson	1000 Bytes	One every 20ms per bus
Office-Substation Traffic	Poisson	20 Bytes	One every 4ms per bus

3.4.3 SPS, Generator and Load Agent Configuration

The SPS uses three types of agents: SPS decision agents, generator agents and load agents. Load and generator agents perform three basic tasks. The load and generator agents monitor the attached bus, push observations to the SPS decision agents and execute commands received from SPS decision agents. SPS decision agents perform two basic tasks. They monitor the power gird for large disturbances requiring SPS actions and issue SPS commands to the load and generator agents. The special protection nodes utilize the communications network to receive system observations from load and generator nodes, to establish and maintain reputation based trust with load and generator nodes, as well as the other special protection nodes, to detect special protection disturbances, to coordinate special protection actions and to execute special protection strategies. The research only evaluates one possible configuration of load, generator and special protection nodes. The NS2 network simulator provides the simulated communications network for the transmission and routing of SPS observations and commands. Figure 4 shows the logical layout of the communications network used in this simulation.

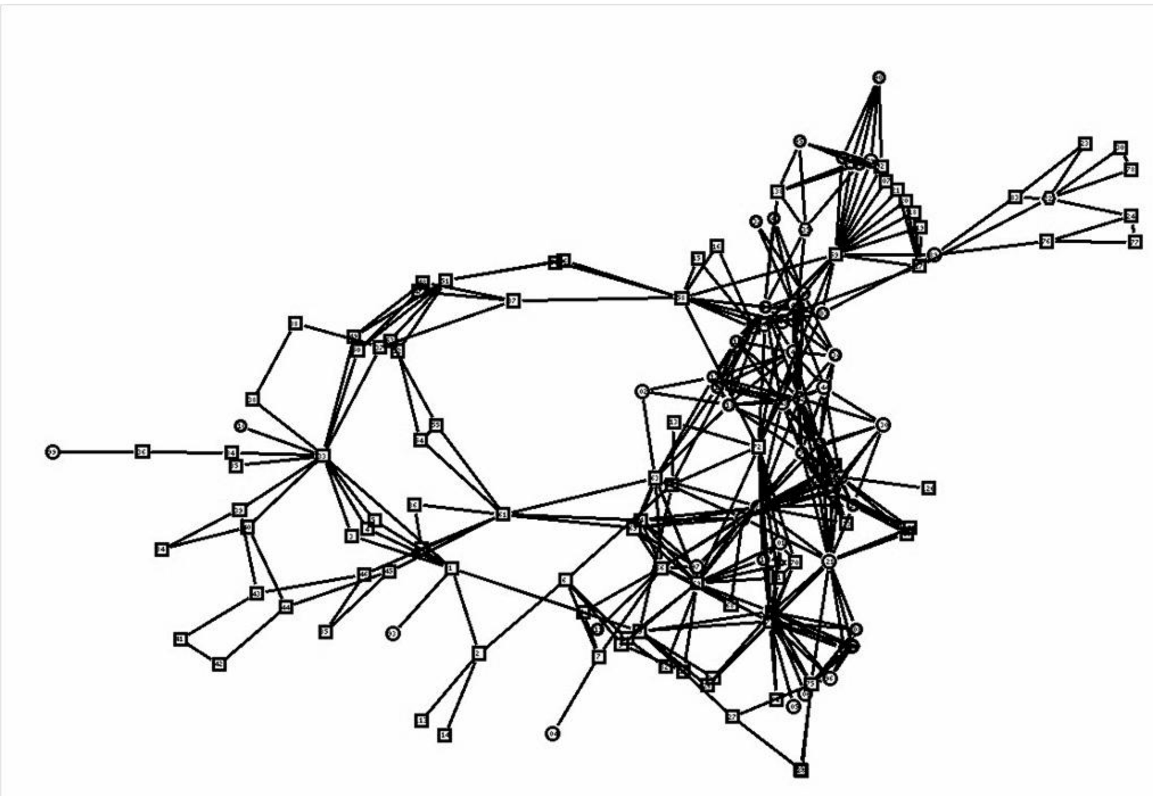

Figure 4. Logical Layout of the Communications Network

3.4.4 SPS Schemes

The special protection scheme provides the coordination and adaptation of the systems special protection strategy to match the actual special protection conditions and is the Component Under Test (CUT). The SPS scheme is the service provided by this system. The ideal special protection service exactly matches system response to a disturbance utilizing the lowest cost strategy. The SPS scheme in this stage of the research monitors all 30 load nodes for trust and all agents malfunctioning or disrupted by the adversary are detectable. The scenario uses a pedagogical abuse case focused on detecting improper reporting of system frequency during updates. However, the behavior of the trust mechanism is not dependent on this specific abuse case, only that the effects of the abuse case can be observed or reported. The SPS scheme requires system updates from the load and generator nodes every 2 ms. Every 6 ms the SPS scheme requires a digest update from system components with the data from the last 60 ms. The digest updates allow the SPS scheme to reconstruct past system states caused by data lost due to background traffic or malicious disruption of the communication network. Finally, the SPS scheme in the first three stages of the research issues load shedding commands to the 12 trusted load agents with the highest loads to fairly distribute the load shed requirements throughout the power grid.

The minimum level of success for an SPS scheme is the ability to maintain system stability without system parameters reaching critical levels. If the system stability reaches critical levels, the probability of the power grid becoming unstable increases. An unstable power grid can cause loss of synchronization resulting in uncontrolled islanding and widespread blackouts. System frequency is the critical system characteristic measured in this research. The critical frequency in this system is 58.8 Hz. Probability of special protection failure increases to unacceptable levels when the system frequency falls below 58.8 Hz. [39]

The SPS decision agents utilize Equation 1 to estimate the steady state frequency resulting from a disturbance, and then to determine the amount of load shedding required to maintain a predetermined frequency while taking into account the normal operation of the generators control systems. [51]

$$\boldsymbol{P_d = P_a + \Delta P_e(\omega_{0+} - \omega_{0-}, \mu_{0+} - \mu_{0-})} \tag{1}$$

> *Formula (1) shows that the size of the disturbance, P_d, is equal to the system accelerating power, P_a , which is proportionate to the change in the system's frequency, plus the change in electrical power demand ΔP_c due to the variation in frequency and voltage. P_d is the key to determining the amount of generation that has been lost. It is important to note that 0- and 0+, respectively, denote the time immediately before and after the disturbance. P_a and ΔP_c can both be obtained based on wide area measurements using the generators' operating status and samples of the system's frequency before and after the disturbance, but measurements must be simultaneously taken at points throughout the region.* [51]

Special protection failures stem from several causes. First, a special protection system can fail to determine an appropriate strategy. An inappropriate strategy does not shed the required load and the frequency drops below 58.8 Hz. This failure can stem from multiple root causes. The system may have a poor special protection scheme or algorithm. The system may also rely on bad or missing data to determine the special protection strategy. Second, a failure can result from an appropriate strategy executed by a system that fails to react to the system disturbance quickly enough. This failure can be caused by a poor special protection scheme or network delays and losses. Third, a special protection failure can result from an appropriate strategy if the load nodes fail to execute commands. Primarily, this failure can result from network delays and losses or from poorly performing trust mechanisms. In this system, communication delays and losses model normal network behaviors, malicious attacks and equipment malfunctions.

3.4.5 Adversarial Scheme

This stage of the research continues previous communication enabled SPS trust research by limiting the adversary to disrupting a maximum of 15 agent, or 50% of the agents in the system. This allows for an easier comparison to the previous research. [52] In this scenario, the SPS must shed approximately 700 MW of power in order to maintain the critical frequency. Table 6 illustrates and highlights that an adversary that strategically disrupts 18 or more agents can prevent the SPS from shedding the minimum 700 MW of power, always disrupting the SPS strategy.

The adversary in the first stage of the research randomly disrupts zero, five, ten or 15 of the load agents. In the second stage the adversary disrupts zero, five, ten or 15 percent of the communication. In the third stage of the research the adversary disrupts a proportional combination of zero, five, ten or 15 agents and zero, five, ten or 15 percent of the communication. The amounts of communication disruption were selected to challenge the data retransmission mechanisms, but to not require a mechanism for estimating missing information.

The adversary in this scenario disrupts the agents by reporting the wrong frequency and by failing to perform SPS commands. The abuse case used by untrusted agents represents a pedagogical abstraction of possible actions taken by a malicious agent attempting to disrupt a communication enabled SPS. Developing additional abuse cases is not a focus of this research.

Table 6. System Loads in MW Highlighting Adversaries Critical Values

Node	123	84	85	133	34	35	51	88	81
Load (MW)	15.28	24.30	27.40	30.85	45.05	49.19	58.45	69.00	82.20
Load Available to Shed	0.00	15.28	39.58	66.98	97.83	142.88	192.07	250.52	319.52
# Disrupted	30	29	28	27	26	25	24	23	22
Node	78	70	71	64	65	83	138	58	86
Load (MW)	89.00	97.42	103.06	113.96	113.96	118.76	140.19	193.63	206.45
Load Available to Shed	401.72	490.72	588.14	691.20	805.16	919.12	1037.88	1178.07	1371.70
# Disrupted	21	20	19	18	17	16	15	14	13
Node	75	66	14	59	63	69	74	27	72
Load (MW)	320.00	333.20	500.00	607.53	914.04	976.64	1025.90	1050.22	1098.00
Load Available to Shed	1578.15	1898.15	2231.35	2731.35	3338.88	4252.92	5229.56	6255.46	7305.68
# Disrupted	12	11	10	9	8	7	6	5	4
Node	73	120	25						
Load (MW)	1318.00	1607.20	1698.74						
Load Available to Shed	8403.68	9721.68	11328.88	13027.62					
# Disrupted	3	2	1	0.00					

3.5 Performance Metrics

This research determines whether the distributed decision making SPS's strategy successfully maintains system stability when faced with an adversary's disruption strategy. The primary metric for determining success or failure is the system frequency. The critical frequency for this system is 58.8 Hz. A system that maintains a frequency greater than 58.8 Hz successfully maintains stability with a high enough level of probability. If the frequency drops below 58.8 Hz, the special protection scheme failed to maintain system stability with a high enough probability.

In addition to frequency, another important metric is cost. Any load shed greater than required to maintain the frequency above 58.8 Hz results in increased cost. While an agent must maintain the minimum frequency to demonstrate overall success, an SPS that minimizes cost achieves a higher level of success compared to SPS that maintains the minimum frequency at a higher cost. The amount of excess load shed is directly related to the amount the final frequency is greater than 58.8 Hz. Additionally, the failure to maintain 58.8 Hz can be quantified as the cost of load shedding every load in the system with additional penalty costs related to the economic impact of a large scale power blackout.

Additional metrics related to the performance of sub-processes also contribute to the analysis of the distributed SPS. Response time is an important sub metric. This SPS requires time to observe the system state and develop trust determinations for the generator and load agents. The SPS must determine and execute the SPS strategy within about 300-400 milliseconds or the frequency drops below 58.8 Hz before the execution of the SPS strategy.

3.6 Experimental Design

The first two stages of the research use a full-factorial design. Stage one and two of the research has one factor with four levels and one factor with two levels. Stage one has four levels of disrupted agents and operates with and without an SPS trust mechanism. Stage two has four levels of network traffic loss and operates with and without an SPS trust mechanism. Therefore, the first two stages of the research require eight experiments each. The third stage of the research uses a fractional-factorial design. There are two factors with four levels that are proportional to each other and one factor with two levels. Stage three has four levels of disrupted agents and four levels of network loss operating with and without an SPS mechanism. Therefore, the third stage of the research requires eight experiments. Results from each stage are analyzed using Tukey's Honest Significant Difference test to provide an ANOVA analysis between each experimental configuration and with standard ANOVA tests between each experimental configuration. [67]

NS2 has predefined 64 good random seed values in the rng.cc file for computer simulation experiments. These random seed values are equally spaced around a 2^{31} cycle of random numbers, where each seed value is approximately 33,000,000 elements apart from each other. [62] The seeds are selected from the rng.cc file to match past research to aid a more direct comparison of simulation results with each replication of the experiment utilizing a unique seed.

3.6.1 Stage One Design

The pilot study for stage one used 36 observations to provide the data required for determining the minimum sample size required to meet accuracy requirements. Additionally the data from the pilot studies provides the data to demonstrate statistical significance in the performance of different SPS scheme compared to no SPS protection schemes and differences in the SPS's response to different experimental factors. Figure 5 and Figure 6 provide a histogram and a Q-Q Plot of the pilot study. The histogram and the Q-Q Plot reveal some minor deviation from normal with a few higher frequency outliers. A Shapiro-Wilk normality test confirms the deviation from normal with a p-value of 0.05573 and a W value of 0.9413. [68] The null hypothesis for the Shapiro Wilk test is that the sample was drawn from a normally distributed population. The W value of 0.9413 is close to one and supports the null hypothesis. At the 95% confidence interval, the sample's p-value just above 0.05 results in the overall acceptance of the null hypothesis. However, the low p-value level make acceptance questionable. The population distribution appears to have a stronger central tendency than normal and skew toward higher frequencies.

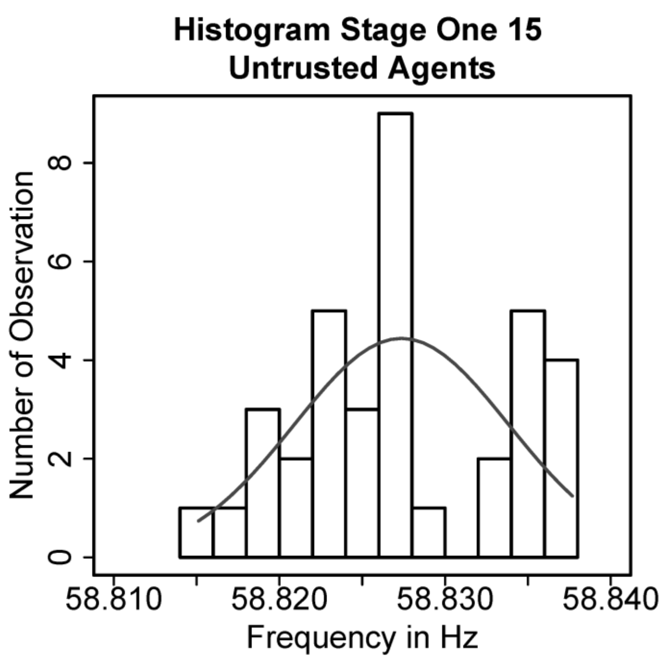

Figure 5. Pilot Simulation Histogram for Stage One (15 Untrusted Agents)

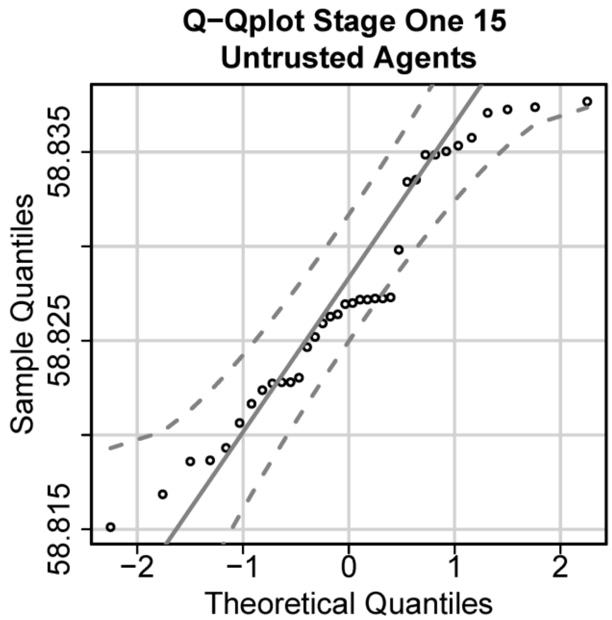

Figure 6. Pilot Simulation Q-Q Plot w/ 95% Confidence Interval for Stage One (15 Untrusted Agents)

Because the goal of the SPS strategy is primarily to determine if the minimum frequency remains above 58.8 Hz, the weak result from the normality test should not negatively impact the statistical significance of the results. Therefore, Equation 2 is used to determine the minimum number of replications required to reach a 99% confidence interval for determining the mean of the simulation results. To compensate for deviation from normal the number of replications is significantly greater than the results from Equation 2. The maximum error is determined from the pilot simulations. The mean frequency from the pilot simulation is 58.82737 Hz with a minimum frequency of 58.81512 Hz. The maximum error (*E*) = 0.0075 is selected by using approximately one half the difference between the minimum frequency and the critical frequency (58.8 Hz). Additionally, the standard deviation for the pilot simulation is 0.006467015. The Z value used for 99% confidence interval is 2.58. Equation 6 determines the minimum number of replications is five, and this research uses 36 replications. This results in 288 simulation trials for the main research.

$$E = z\sigma_{\bar{x}} \rightarrow n = \frac{z^2\sigma^2}{E^2} \rightarrow 4.94908 = \frac{2.58^2 * 0.006467015^2}{0.0075^2} \tag{2}$$

3.6.2 Stage Two Design

The pilot study for stage two used 36 observations to provide the data for determining the minimum sample size needed to meet accuracy requirements. Additionally, the pilot studies provide the data to demonstrate statistical significance in the performance of different SPS schemes compared to no SPS protection schemes and differences in the SPS's response to experimental factors. Figure 7 and Figure 8 provide a histogram and a Q-Q Plot of the pilot study. The histogram and the Q-Q Plot reveal some minor deviations from normal with a flatter response. However, the Shapiro-Wilk normality test indicates the sample is taken from a normal distribution with a p-value of 0.4752 and a W value of 0.9717. [68] The null hypothesis for the Shapiro Wilk test is that the sample was drawn from a normally distributed population. The W value of 0.9717 is close to one and supports the null hypothesis. At the 95% confidence interval, the sample's p-value above 0.05 results in the acceptance of the null hypothesis.

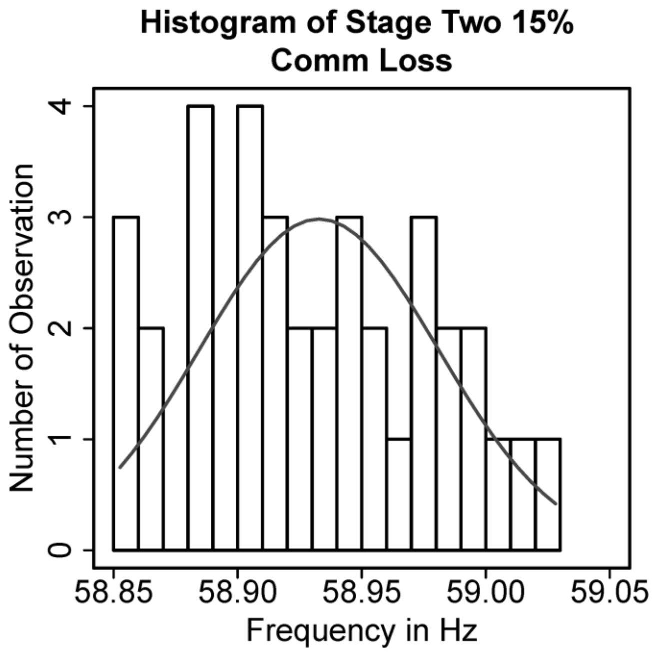

Figure 7. Pilot Simulation Histogram for Stage Two (15% Communication Loss)

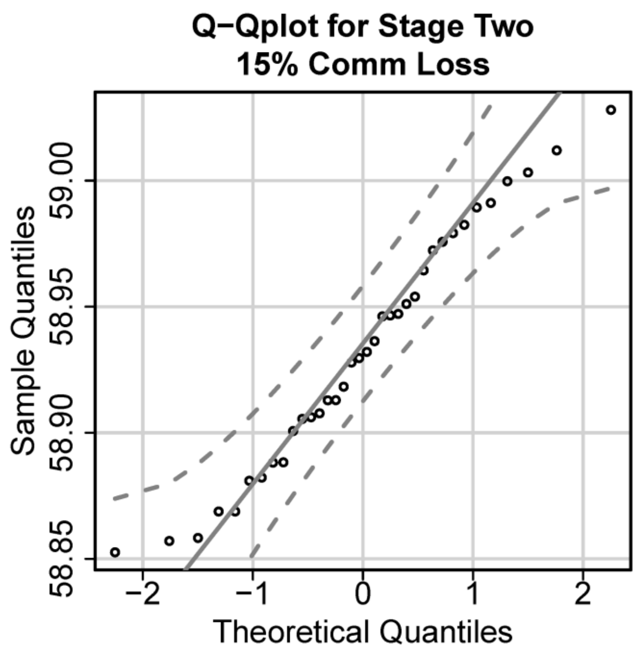

Figure 8. Pilot Simulation Q-Q Plot w/ 95% Confidence Interval for Stage Two (15% Communication Loss)

Because the pilot study indicates the population is normally distributed, Equation 3 is used to determine the minimum number of replications required to reach a 99% confidence interval for determining the mean of the simulation results. The maximum error is determined from the pilot simulations. The mean frequency from the pilot simulation is 58.93276 Hz with a minimum frequency of 58.85262 Hz. The maximum error (E) = 0.025 is selected by using approximately one-half the difference between the minimum frequency and the critical frequency (58.8 Hz). Additionally, the standard deviation for the pilot simulation is 0.04813493. The Z value used for 99% confidence interval is 2.58. Equation 3 determines the minimum number of replications is 25, and this research uses 36 replications to improve the statistical analysis of the experiment. This results in 288 simulation trials for the main research.

$$E = z\sigma_{\bar{x}} \rightarrow n = \frac{z^2\sigma^2}{E^2} \rightarrow 24.6763 = \frac{2.58^2 * 0.04813493^2}{0.025^2} \tag{3}$$

3.6.3 Stage Three Design

The pilot study for stage three used 36 observations to provide the data required for determining the minimum sample size required to meet accuracy requirements. Additionally, the pilot studies provide the data to demonstrate statistical significance in the performance of different SPS schemes compared to no SPS protection schemes and differences in the SPS's response to different experimental factors. Figure 9 and Figure 10 provide a histogram and a Q-Q Plot of the pilot study. The histogram and the Q-Q Plot reveal some minor deviations from normal with a flatter response. However, the

Shapiro-Wilk normality test indicates the sample is taken from a normal distribution with a p-value of 0.4752 and a W value of 0.9717. [68] The null hypothesis for the Shapiro Wilk test is that the sample was drawn from a normally distributed population. The W value of 0.9717 is close to one and supports the null hypothesis. At the 95% confidence interval, the sample's p-value above 0.475 results in the overall acceptance of the null hypothesis.

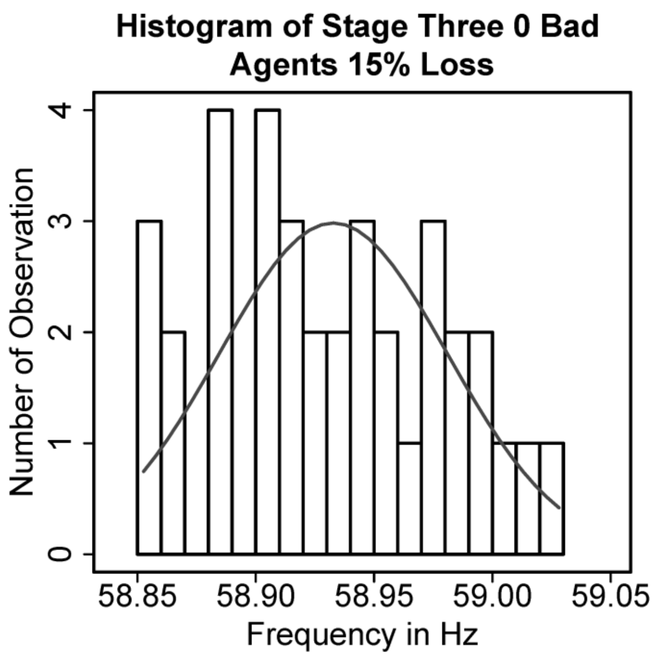

Figure 9. Pilot Simulation Histogram for Stage Three (15% Communication Loss and 0 Untrusted Agents)

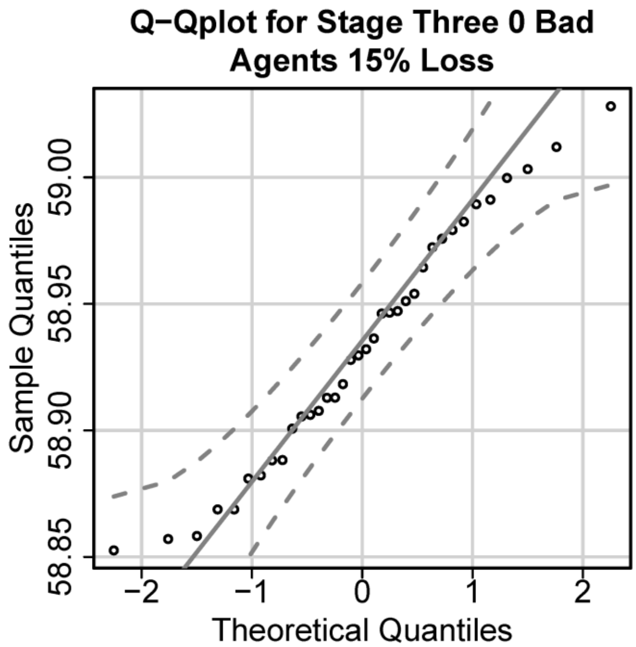

Figure 10. Pilot Simulation Q-Q Plot w/ 95% Confidence Interval for Stage Three (15% Communication Loss and 0 Untrusted Agents)

Because the goal of the SPS strategy is primarily to determine if the minimum frequency remains above 58.8 Hz, any deviation from normality should not negatively impact the statistical significance of the results. Therefore, Equation 4 is used to determine the minimum number of replications required to reach a 99% confidence interval for determining the mean of the simulation results. To compensate for deviation from normal, the number of replications is significantly greater than the results from Equation 4. The maximum error is determined from the pilot simulations. The mean frequency from the pilot simulation is 58.93276 Hz with a minimum frequency of 58.85262 Hz. The maximum error (E) = 0.025 is selected by using approximately one-half the difference between the minimum frequency and the critical frequency (58.8 Hz). Additionally, the standard deviation for the pilot simulation is 0.004813493. The Z value used for 99% confidence interval is 2.58. Equation 4 determines the minimum number of replications is 24, and this research uses 36 replications. This results in 288 simulation trials for the main research. In addition to the main results, the behavior of the trust mechanism is analyzed to show how the trust values vary as the system operates.

$$E = z\sigma_{\bar{x}} \rightarrow n = \frac{z^2\sigma^2}{E^2} \rightarrow 24.6763 = \frac{2.58^2 * 0.04813493^2}{0.025^2} \tag{4}$$

3.7 Methodology Summary

This paper describes the research methodology used to evaluate three distributed decision making communication enabled SPSs. The methodology defines and discusses the power transmission system and the distributed SPSs as the system and component under test. Additionally, the characteristics of the system are analyzed to determine the workloads, metrics, parameters and factors that affect the performance of the system. Simulation is selected as the appropriate evaluation technique and the experimental design required to achieve a 99% confidence interval is identified. This research methodology identifies a method to collect valid data required to evaluate and analyze the performance of the three distributed decision making communication enabled SPSs.

IV. Methodology Stage Four

4.1 Chapter Overview

This research methodology describes the processes used to explore and analyze a proposed Special Protection System (SPS) that addresses system modernization and transmission system reliability directly and other areas of smart grid development indirectly. Specifically, this stage of the research continues the study of applying simple trust based mechanisms to communication enabled SPSs. The previous stages of the research tested the performance of a distributed decision making communication enabled SPS when operating through the disruption of communications and system agents. In the previous stages of the research, the SPS operated with no limitation on the resources available to monitor and protect the system from disruptions caused by malicious actions or malfunctions. The SPSs in the previous stages of the research monitored every node and could detect every disruption.

This stage of research continues by building on the foundation established in the previous stages of the research by adding constraints to the SPS and applying game theory principles. In this final stage of the research, the SPS determines a defensive protection strategy when both the SPS and the adversary have limited resources and must consider costs and utility. The introduction of costs limits the amount and the effectiveness of security monitoring available to the SPS. Because of this, the SPS must strategically select a limited number of agents to monitor.

This stage of the research also includes pilot simulations and analytical analysis of key design decisions including the processes to determine the minimum number of monitored agents required to defend the SPS and the number of loads to shed. The application of realistic limitations on the SPS's monitoring and the adversary's attack is a significant departure from previously explored communication enabled SPSs. By providing a distributed processes relying on game theory, the system provides the potential for increased effectiveness compared to traditional and recently explored SPSs when faced with partially detectable malicious/malfunctioning agents and communication losses.

4.2 Problem Definition

4.2.1 Goals and Hypothesis

This research methodology addresses the last stage of the research and builds upon the foundation established during the previous three stages of the research. This methodology focuses on one specific hypothesis, but seeks to achieve several goals in the process of investigating the hypothesis.

Hypothesis Stage Four:

A distributed decision making communication enabled SPS using resource constrained simple reputation based trust mechanisms can use game theory principles to successfully determine and execute an appropriate SPS load shedding strategy while experiencing various levels of network traffic and losses and various levels of disrupted agents introduced by a resource constrained adversary also using strategy determined from game theory principles.

During this stage of the research, the primary goal is to test the performance of a distributed SPS when faced with cost limitations in terms of how many generator and load agents can be monitored by a trust mechanism and with limitations in the ability of the trust mechanism to detect untrustworthy agents. A supporting goal is the assessment of a game theoretic approach to determine a generator and load monitoring strategy that reduces uncertainty of the system state to a level required to produce a reliable load shedding strategy. A second supporting goal is to test a stochastic decision process that can determine a load shedding strategy from the beliefs about the system state with the uncertainty left by the monitoring strategy.

A minimum level of success for the SPS is defined by the SPS detecting the system disturbance and then maintaining system stability by shedding load quickly enough and accurately enough to preventing the system frequency from dropping below the critical level. Increased success results from minimizing the cost of the SPS strategy. The cost is minimized by shedding the minimum amount of load required to maintain the system frequency above the critical level. Additionally, the degree of success is measured by comparing the distributed SPS agent's performance to an undefended SPS. Finally, the results from the experiments are compared to the results from the previous three stages of the research.

Testing these research hypotheses drives significant changes from the basic operation of traditional SPSs. A traditional SPS does not utilize an adaptive approach to maintain system stability. Traditional SPSs protect system components from damage and can prevent large scale blackouts under predetermined scenarios. The pre-coordinated strategy does not result in optimization of the protective actions. The traditional SPS's lack of dynamic strategy often results in suboptimal capacity shedding. [37] Suboptimal shedding results in the rejection of more load than required increasing cost, or less load than required increasing the probability of widespread uncontrolled blackouts. A traditional SPS also fails to consider other factors such as trustworthiness of system components. Rather than a script to deal with predicted disturbances, a communication enabled SPS reacts dynamically to the system state while considering many factors not considered by a traditional SPS.

In addition to changes from traditional SPSs, the research hypothesis also drives changes from the operation of recently researched centralized decision making communication enabled SPSs and the operation of the SPSs in the last three stages of this research. Past research and the previous three stages of this research assumed all untrustworthy agents could be detected and that the trust mechanism could be used to monitor all of the generator and load nodes. [52] [59] [51] Compared to the previously researched distributed SPSs, the revised SPS relying on game theory requires an agent monitoring strategy and a revised load shedding strategy to deal with the lack certainty in the untrusted agent detection. Finally, the introduction of uncertainty changes the SPS load shedding strategy from a deterministic to a probabilistic process.

Although there are some advantages to the centralized SPS in terms of network capacity and equipment costs, the distributed decision making SPS should have the advantage over both traditional and the centralized SPS in terms of reliability and security. As discussed above, a traditional SPS does not rely on any active coordination/adaptation to operate. This lack of coordinated adaptation results in fewer network or communication security vulnerabilities in the determination of an SPS strategy. However, the lack of coordination also reduces the reliability of the traditional SPS by reducing the number of scenarios an SPS can successfully recover from. Additionally, the lack of coordination prevents the detection of untrustworthy nodes, resulting in the possibility that nodes fail to execute SPS commands and the SPS fails to maintain system stability. The reliance on predetermined actions to match possible disturbances increases the probability of cascading failures compared to coordinated communication enabled SPSs. [39] When comparing the distributed decision making communication enabled SPS to the centralized decision making communication enabled SPS, removing the centralized decision agent from being a single point of failure will likely further increase the reliability and security of the power grid. Additionally, when compared to traditional SPSs and previous examples of centralized decision making communication enabled SPSs, the distributed decision making SPS agent using game theory should be successful when operating in a wider range of realistic conditions including levels of uncertainty.

4.2.2 Approach

For practical reasons, power transmission systems require SPS. System malfunctions can create unstable conditions or disturbances. When disturbances cannot be corrected with normal system processes, the system either successfully employs protection systems, including SPSs, or risks catastrophic failure. A catastrophic failure in a power transmission grid results in widespread islanding, blackouts and possible equipment damage. The 1965 and 2003 blackouts illustrate extreme examples of what happens when multiple protection systems, including SPSs, fail to successfully react to disturbance and keep the power grid stable. [60] [61]

This research utilizes a scenario that creates a realistic special protection condition and evaluates the distributed SPS's ability to return the system to a stable operation. The creation of a realistic special protection condition requires extensive electric transmission grid knowledge. In this research scenario, a disturbance requiring special protection actions is created by introducing system failures and other faults. The failures and faults create a disturbance resulting in an imbalance requiring generators to be removed from service. The sudden removal of generation capacity from the power grid creates the disturbance that requires SPS load shedding actions. Based on data gleaned from past large scale blackouts, the conditions created produce a realistic SPS disturbance. [4]

To demonstrate acceptable response to system disturbances, the research seeks to test the system operating over a data network with a variety of operating conditions and workloads. The research methodology evaluates the distributed SPS's ability to operate in an unsecure and imperfect environment by introducing system malfunctions that could be caused by malicious actions or malfunctioning components. The SPS relies on simple reputation-based trust mechanisms and game theory to determine and execute the actions required to maintain system stability.

In order to test a special protection scheme, scenarios requiring a special protection intervention must be created in the simulation. However, this research is limited to evaluating a single scenario and does not address the SPS's ability to respond to alternate special protection conditions. The danger of developing a system that performs correctly for only one scenario is a significant limitation on this research. The research attempts to keep the distributed SPS's action general enough to respond to any SPS action that requires load shedding.

4.3 Testing Environment

The primary task in the fourth stage of this research is the development and testing of an agent based communication enabled SPS with distributed decision making agents using game theory and reputation based trust mechanisms. The testing determines the SPS's ability to successfully maintain stability of the power grid when experiencing a significant disturbance that could result in an uncontrolled cascading blackout and while experiencing malfunctions and malicious activities.

A federation of network and power simulation provides the primary evaluation method for the testing of the distributed special protection system. In this circumstance, the selection of the simulation environment stems from rational determination and circumstance. First, much of the infrastructure to enable smart grid technologies is not in place. Even the few areas where a limited smart grid capacity exists, experimenting with operational power transmission systems introduces excessive risk and cost. When modeling a regional power transmission grid, no reliable analytic models exist for measuring the interactions between power transmission systems and the coordination enabled by smart grid technologies and data networks. The tool that enables the development and the study of this SPS is a realistic simulation environment for both the power system and the communications network. The simulation environment selected for this research is the combination of the PSS/E power simulator and the NS2 network simulator federated together by the Electric Power and Communication Synchronizing Simulator (EPOCHS). [50] [62] Figure 2 illustrates the basic configuration EPOCHS simulation environments. [51] Inside these simulation programs, specific power transmission and network models provide a realistic and validated test environment. Using this environment also provides the opportunity to compare the results of new research with existing research efforts. [52] [51] [59]

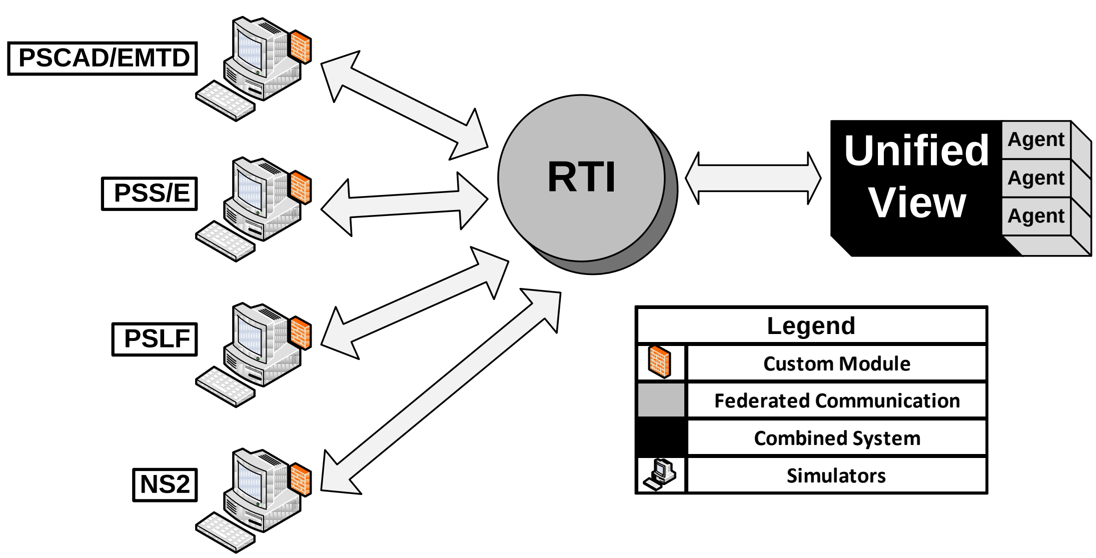

Figure 11. Graphical Representation of EPOCHS Simulation Environments [59]

Each simulation run utilizes the same basic scenario. Power transmission lines are tripped due to malfunction and overloading to create a system imbalance that requires the removal of a specific generator from the system. This results in an imbalance and creates an unstable system condition with a dropping system frequency. The distributed

SPS uses the data network to determine and execute an SPS strategy to reestablish system stability by intelligently shedding load. The simulation runs for 50 seconds in the simulation environment. The factors utilized in the simulation include levels of communication loss and the location of the untrusted nodes. The research utilizes the same randomization seeds as in previous research to better correlate results. An analysis of variance and a comparison of confidence intervals are used to determine the statistical significance of the simulation results. [63]

4.4 Special Protection Test Details

The SPS test case scenario operates within system boundaries and includes the system services, the system under test, the workload the system operates under and the factors that are controlled to test and evaluate the component under test. The component under test is the SPS scheme, and each stage of the research evaluates a specific scheme's response to the testing factors. The system under test includes power transmission grid, the communications network, the load and generator nodes, the special protection nodes and the distributed special protection scheme.

4.4.1 Power Transmission Configuration

The power transmission grid provides the physical connections between generator, load nodes and other transmission system components. This research only uses one power transmission configuration. The configuration used is a modified IEEE 145-bus 50 generator test case to represent the power transmission system. [64] Modification to the original test case changes the behavior of a few generators, adds an additional power transmission line, reduces the overall generation capacity and rebalances power flows in order to increase the importance of the power flowing over key transmission lines. [51] The degree of interconnection between the nodes in the system influences the system's ability to maintain stability during disturbances. A well connected electrical grid provides more flexibility for transferring power and maintaining stability, but often contains interconnections that are not capable of transporting enough power to maintain stability during special protection situations. [39] This research models a well-connected electric transmission grid. Additional changes to the electrical transmission grid are outside the scope of this research. The IEEE test case is used in PSS/E to model transient stability during the simulated SPS actions. Figure 12 shows the logical layout of the Power Grid used in this simulation

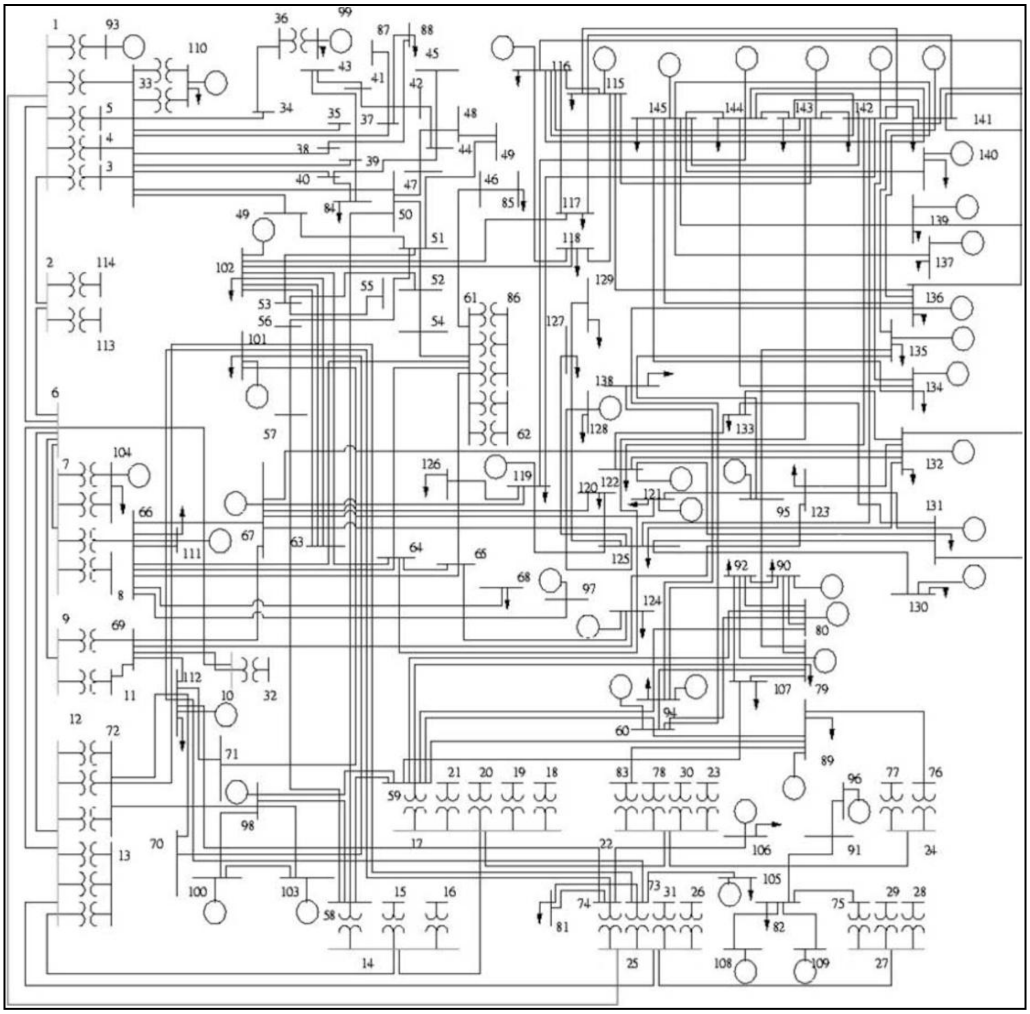

Figure 12. Logical Layout of the Power Grid [51]

The power transmission system operates at a specific workload described by the amount of power generated, the amount of power required by the loads and the amount of transmission capacity on each power transmission line. As a power transmission grid is operated closer to maximum efficiency and minimum safety levels, less reserve capacity remains. [39] In addition, larger systems have more flexibility in dealing with disturbance than a smaller system where there may be very few strategies for maintaining system stability. In a stable system, the power generated and the power required for the loads are in balance and the transmission lines are within normal operational limits. When the power generation capacity and the system load requirements do not balance, or transmission lines operate outside of normal operational limits, the system becomes unstable. Power generation and transmission systems have methods to adjust for fluctuations in power generation capacity and load requirements. A system disturbance in this research is a condition that creates an imbalance between the generation capacity, the system load and transmission line capacity too large for normal system processes to maintain stability. This simulation utilizes a power generation and load imbalance along with overloaded transmission lines to create a disturbance that requires an SPS to maintain system stability.

4.4.2 Communication Network Configuration

The communication network provides the logical connections between system nodes. The load and generator nodes utilize the communications network to share local system observations and to receive commands. The number and location of the generator and load nodes and data link capacity influences the performance of the system. This research only observes one logical communication network configuration. Additionally, the data link capacity used in this research is 100 Mbps, representing the lower boundary of expected capability for future smart grid networks and is the minimum capacity required for this SPS to operate. [65] The agent based communication enabled SPS's communication network infrastructure closely mirrors the power transmission grid based on an assumption that future smart grid networks will likely run along the same routes as the power transmission systems. [37] [53] In a smart grid, the physical and logical design of the data network influences the performance and reliability of a data network. [32]

The operation of the communication network provides a workload used to test the SPS schemes. The network workload for this system includes the background network traffic, the amount of packet loss due to malicious actions or malfunctions and the number, location and detection probability of untrusted nodes in the system. The background traffic models traffic that may occur at different times in a communication network used for SCADA type traffic. The background network traffic for this research is modeled from an analysis of LAN and SCADA network traces and assumption about the utilization of future smart grid networks. [59] However, the traffic differs significantly from the traffic used in previous research with a higher probability of background traffic occurring during the critical first 300-350 ms of the simulation. Additionally, non-power related traffic is not used. Background traffic and communication losses influence the performance of the distributed SPS. Table 7 shows the background traffic utilized by this research. As background traffic and losses increase, delays in the network increase and reliability of the network decreases. [66] Without appropriate mechanisms to overcome delays and loss, the distributed SPS can fail to meet the minimum timing requirements or fail to obtain enough data to develop an SPS. The background traffic in this simulation uses the same background traffic mechanisms used in previous research with higher occurrence rates and modified packet sizes. The traffic falls between the medium and high levels from. [59]

Table 7. Background Traffic Rates [66]

Background Traffic Type	Distribution	Packet Size	Rate
SCADA	Constant	44 Bytes	One every 4ms per bus
Power Quality Data	Poisson	76-196 Bytes	One every 10ms per bus
Routine Internal Traffic	Poisson	1000 Bytes	One every 20ms per bus
Office-Substation Traffic	Poisson	20 Bytes	One every 4ms per bus

4.4.3 SPS, Generator and Load Agent Configuration

The SPS uses three types of agents: SPS decision agents, generator agents and load agents. Load and generator agents perform three basic tasks. The load and generator agents monitor the attached bus, push observations to the SPS decision agents and execute commands received from SPS decision agents. SPS decision agents perform two basic tasks. They monitor the power gird for large disturbance requiring SPS actions and issue SPS commands to the load and generator agents. The special protection nodes utilize the communications network to receive system observations from load and generator nodes, to establish and maintain reputation based trust with load and generator nodes as well as the other special protection nodes, to detect special protection disturbances, to coordinate special protection actions and to execute special protection strategies. The research only evaluates one possible configuration of load, generator and special protection nodes. The NS2 network simulator provides the simulated communications network for the transmission and routing of SPS observations and commands. Figure 13 shows the logical layout of the communication network used in this simulation.

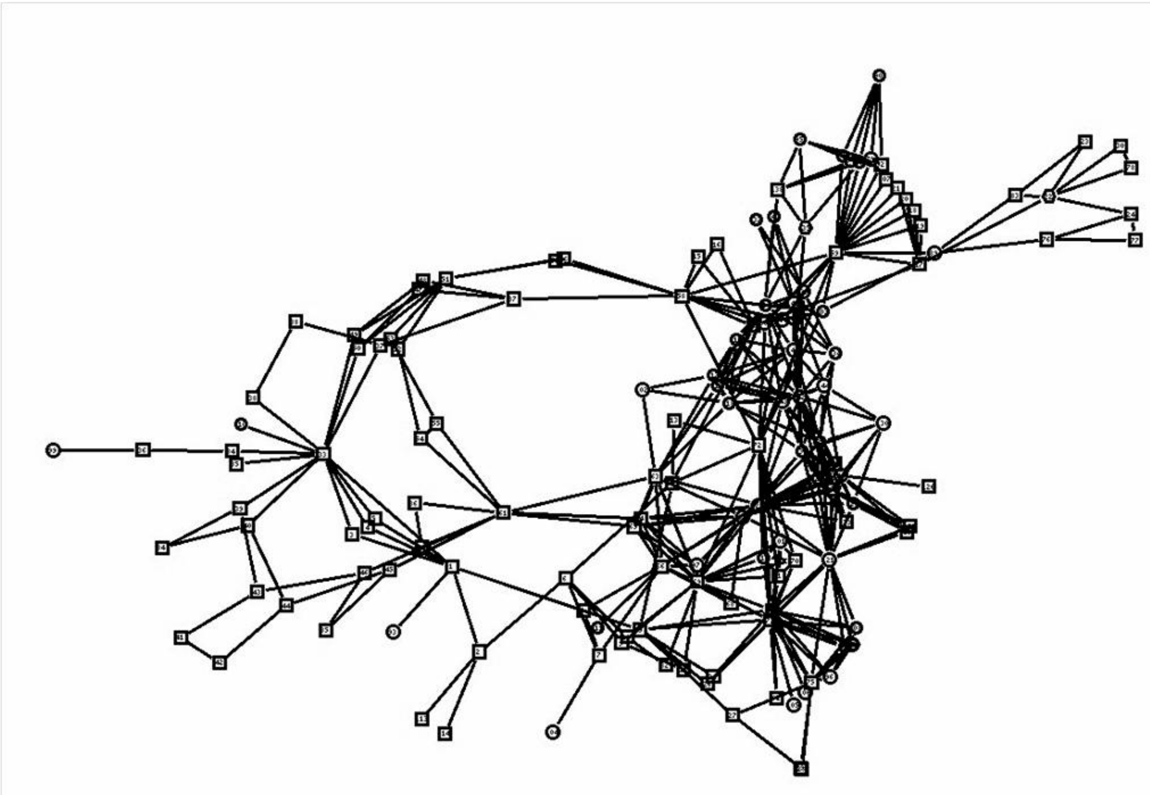

Figure 13. Logical Layout of the Communications Network

4.4.4 SPS Schemes

The special protection scheme provides the coordination and adaptation of the systems special protection strategy to match the actual special protection conditions and is the Component Under Test (CUT). The SPS scheme is the service provided by this system. The ideal special protection service exactly matches system response to a disturbance utilizing the lowest cost strategy. The research relied on pilot simulations to reinforce analytical results to determine the number of agents the SPS must monitor to assure a high probability of success when dealing with the maximum level of expected disruption from the adversary. The SPS scheme in this stage of the research uses game theory to strategically monitor 22 load nodes with a 90% probability of detecting malfunctioning or disrupted agents. This limitation results in 86,493,225 possible strategies to monitor 30 nodes.[1]

The game formulation for the fourth stage of this research uses several attributes to determine the utility and cost for each of the players' strategies. The SPS player's primary objective is shedding enough power to maintain stability, with the minimization of excess power shed as a secondary objective. The largest influence on the utility and cost for the SPS player is the benefit achieved maintaining system stability. The benefit can be substantial with up to $4-10 Billion saved compared to the estimated losses caused by the August 14, 2003 outage. [60] Even the prevention of more routine SPS failures potentially saves hundreds of thousands of dollars. [36]

Additionally, the game theoretic formulation uses the adversary's limitation of disrupting 15 nodes to determine the minimum number of nodes that must be monitored and to determine the optimal protection strategy. The scenario uses a pedagogical abuse case focused on detecting improper reporting of system frequency during updates. However, the behavior of the trust mechanism is not dependent on this specific abuse case, only that the effects of the abuse case can be observed or reported. The SPS scheme requires system updates from the load and generator nodes every 2 ms. Every 6 ms the SPS scheme requires a digest update from system components with the data from

[1] See Appendix A for detailed explanation of game theory formulation for the SPS's strategy

the last 60 ms. The digest updates allow the SPS scheme to reconstruct past system states caused by data lost due to background traffic or malicious disruption of the communications network. After application of the protection and disruption strategies the SPS uses a stochastic decision process to determine a load shedding strategy taking into account the uncertainty of detecting all of the untrustworthy agents by the SPS's trust monitoring mechanisms. The SPS adjusts the amount of load to be shed and the number of agents to receive the load shed commands. The SPS makes the adjustments based upon the assumption that a predictable number of untrusted agents were not detected and the desire to maintain a minimum of 98.95% probability for successful load shedding.

The minimum level of success for an SPS scheme is the ability to maintain system stability without system parameters reaching critical levels. If the system stability reaches critical levels, the probability of the power grid becoming unstable increases. An unstable power grid can cause loss of synchronization resulting in uncontrolled islanding and widespread blackouts. System frequency is the critical system characteristic measured in this research. The critical frequency in this system is 58.8 Hz. Probability of special protection failure increases to unacceptable levels when the system frequency falls below 58.8 Hz. [39]

The SPS decision agents use Equation 5 to estimate the steady state frequency resulting from a disturbance, and then to determine the amount of load shedding required to maintain a predetermined frequency while taking into account the normal operation of the generators control systems. [51]

$$\boldsymbol{P_d = P_a + \Delta P_e(\omega_{0+} - \omega_{0-}, \mu_{0+} - \mu_{0-})} \tag{5}$$

> *Formula (1) shows that the size of the disturbance, P_d, is equal to the system accelerating power, P_a , which is proportionate to the change in the system's frequency, plus the change in electrical power demand ΔP_c due to the variation in frequency and voltage. P_d is the key to determining the amount of generation that has been lost. It is important to note that 0- and 0+, respectively, denote the time immediately before and after the disturbance. P_a and ΔP_c can both be obtained based on wide area measurements using the generators' operating status and samples of the system's frequency before and after the disturbance, but measurements must be simultaneously taken at points throughout the region.* [51]

Special protection failures stem from several causes. First, a special protection system can fail to determine an appropriate strategy. An inappropriate strategy does not shed the required load and the frequency drops below 58.8 Hz. This failure can stem from multiple root causes. The system may have a poor special protection scheme or algorithm. The system may also rely on bad or missing data to determine the special protection strategy. Second, a failure can result from an appropriate strategy executed by a system that fails to react to the system disturbance quickly enough. This failure can be caused by a poor special protection scheme or network delays and losses. Third, a special protection failure can result from an appropriate strategy if the load nodes fail to execute commands. Primarily, this failure can result from network delays and losses or from poorly performing trust mechanisms. In this system, communication delays and losses model normal network behaviors, malicious attacks and equipment malfunctions.

4.4.5 Adversarial Scheme

This stage of the research continues previous communication enabled SPS trust research by limiting the adversary to disrupting a maximum of 15 agents, or 50% of the agents in the system and up to 15% of the communications on each link. This allows for an easier comparison to the previous research. [52] For purposes of the developing a realistic game model, the level of communication loss from malicious or malfunctioning nodes and the number of disrupted nodes is restricted by the assumption that an adversary has limited resources, and the costs related to disrupting communication prevent higher levels of network disruption. The maximum cost for the adversary is limited by assumptions about the rationality and capability of an adversary discussed in the literature review. These concepts of utility and cost allow the system to be analyzed using game theory. In this scenario, the SPS must shed approximately 700 MW of power in order to maintain the critical frequency. An adversary with limited resources must use the resources strategically to maximize the potential of disrupting the SPS load shedding strategy. Table 8 illustrates and highlights that an adversary that strategically disrupts 18 or more agents can prevent the SPS from shedding the minimum 700 MW of power, always disrupting the SPS strategy.

The adversary in this stage of the research disrupts a proportional combination of zero, five, ten or 15 agents and zero, five, ten or 15 percent of the communication. The adversary selects the agents to disrupt strategically, rather than randomly. This results in one strategy when disrupting zero agents, 142,506 possible strategies when disrupting five agents, 30,045,015 possible strategies when 10 agents are attacked and 155,117,520 possible strategies when 15 nodes are attacked.[2] The amounts of communication disruption were selected to challenge the data retransmission mechanisms, but to not

[2] See Appendix A for detailed explanation of the game theory formulation for the adversary's strategy.

require a mechanism for estimating missing information. The adversary builds its agent disruption strategy knowing that the SPS does not monitor every agent, but the adversary does not know exactly how many agents are monitored. The adversary builds the strategy achieve maximum utility by causing the system frequency to drop below the critical level of 58.8 Hz. Any utility gained by increasing the amount of load shed by the SPS is coincidental.

The adversary in this scenario disrupts the agents by reporting the wrong frequency and by failing to perform SPS commands. The abuse case used by untrusted agents represents a pedagogical abstraction of possible actions taken by a malicious agent attempting to disrupt a communication enabled SPS. Developing additional abuse cases is not a focus of this research.

Table 8. System Loads in MW Highlighting Adversaries Critical Values

Node	123	84	85	133	34	35	51	88	81
Load (MW)	15.28	24.30	27.40	30.85	45.05	49.19	58.45	69.00	82.20
Load Available to Shed	0.00	15.28	39.58	66.98	97.83	142.88	192.07	250.52	319.52
# Disrupted	30	29	28	27	26	25	24	23	22
Node	78	70	71	64	65	83	138	58	86
Load (MW)	89.00	97.42	103.06	113.96	113.96	118.76	140.19	193.63	206.45
Load Available to Shed	401.72	490.72	588.14	691.20	805.16	919.12	1037.88	1178.07	1371.70
# Disrupted	21	20	19	18	17	16	15	14	13
Node	75	66	14	59	63	69	74	27	72
Load (MW)	320.00	333.20	500.00	607.53	914.04	976.64	1025.90	1050.22	1098.00
Load Available to Shed	1578.15	1898.15	2231.35	2731.35	3338.88	4252.92	5229.56	6255.46	7305.68
# Disrupted	12	11	10	9	8	7	6	5	4
Node	73	120	25						
Load (MW)	1318.00	1607.20	1698.74						
Load Available to Shed	8403.68	9721.68	11328.88	13027.62					
# Disrupted	3	2	1	0.00					

4.5 Performance Metrics

This research determines whether the distributed decision making SPS's strategy successfully maintains system stability when faced with an adversary's disruption strategy. The primary metric for determining success or failure is the system frequency. The critical frequency for this system is 58.8 Hz. A system that maintains a frequency greater than 58.8 Hz successfully maintains stability with a high enough level of probability. If the frequency drops below 58.8 Hz, the special protection scheme failed to maintain system stability with a high enough probability.

In addition to frequency, another important metric is cost. Any load shed greater than required to maintain the frequency above 58.8 Hz results in increased cost. While an agent must maintain the minimum frequency to demonstrate overall success, an SPS that minimizes cost achieves a higher level of success compared to an SPS that maintains the minimum frequency at a higher cost. The amount of excess load shed is directly related to the amount the final frequency is greater than 58.8 Hz. Additionally, the failure to maintain 58.8 Hz can be quantified as the cost of load shedding every load in the system with additional penalty costs related to the economic impact of a large scale power blackout.

Additional metrics related to the performance of sub-processes also contribute to the analysis of the distributed SPS. Response time is an important sub metric. This SPS requires time to observe the system state and develop trust determinations for the generator and load agents. The SPS must determine and execute the SPS strategy within about 300-400 milliseconds or the frequency drops below 58.8 Hz before the execution of the SPS strategy.

4.6 Experimental Design

This final stage of the research utilizes a fractional-factorial design. There are four factors in the fourth stage of the research. Two factors have four levels that are proportional to each other as constrained by the adversary’s strategy, one factor with 155,117,520 possible levels and one factor with 5852925 possible levels. However, separate analyses of the game formulation reveals dominate strategies for both the SPS and the adversary given the stated assumption concerning cost and utility. Using game theory concepts the third factor can be reduced to one dominate strategy. Additionally, game theory concepts can reduce the fourth factor to four dominate strategies with each of the strategy dependent on the level selected in the second factor (number of nodes attacked). This results in the need for 8 experiments, 4 without the SPS strategy monitoring load agents and 4 with the SPS strategy monitoring the selected load agents. Results from this stage of the research are analyzed using Tukey's Honest Significant Difference test to provide an ANOVA analysis between each experimental configuration and with standard ANOVA tests between each experimental configuration. [67]

NS2 has predefined 64 good random seed values in the rng.cc file for computer simulation experiments. These random seed values are equally spaced around a 2^{31} cycle of random numbers, where each seed value is approximately 33,000,000 elements apart from each other. [62] The seeds are selected from the rng.cc file to match past research to aid a more direct comparison of simulation results with each replication of the experiment utilizing a unique seed.

The pilot study used 64 observations to provide the data required for determining the minimum sample size required to meet accuracy requirements. Additionally the data from the pilot studies provides the data to demonstrate statistical significance in the performance of different SPS schemes and differences in the SPS's response to different experimental factors. Figure 14 and Figure 15 provide a histogram and a Q-Q Plot of the pilot study. The histogram and the Q-Q Plot reveal some minor deviation from normal with a few higher frequency outliers. A Shapiro-Wilk normality test confirms the deviation from normal with a p-value of 0.002076 and a W value of 0.9107. [68] The null hypothesis for the Shapiro Wilk test is that the sample was drawn from a normally distributed population. The W value of 0.9107 is close to one and supports the null hypothesis. At the 95% confidence interval, the sample's p-value less than 0.05 results in the overall rejection of the null hypothesis. The population distribution appears to have a stronger central tendency than normal with a higher frequency outlier.

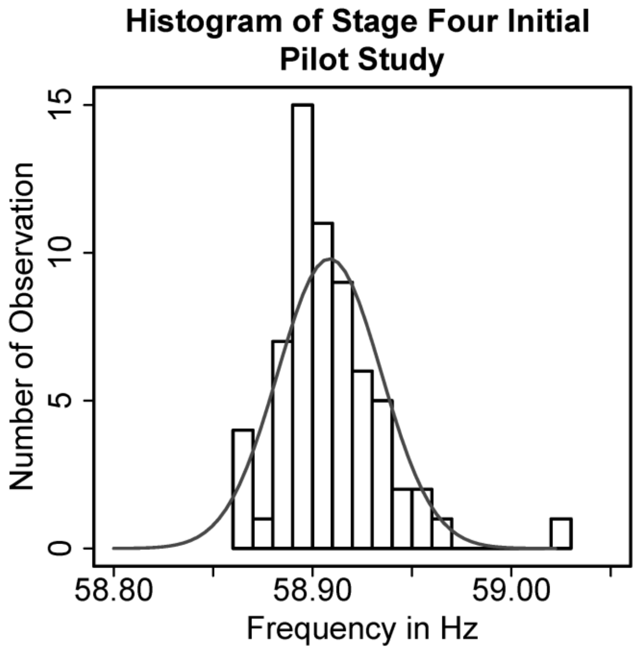

Figure 14. Pilot Simulation Histogram for Stage Four (15% Communication Loss and 0 Untrusted Agents)

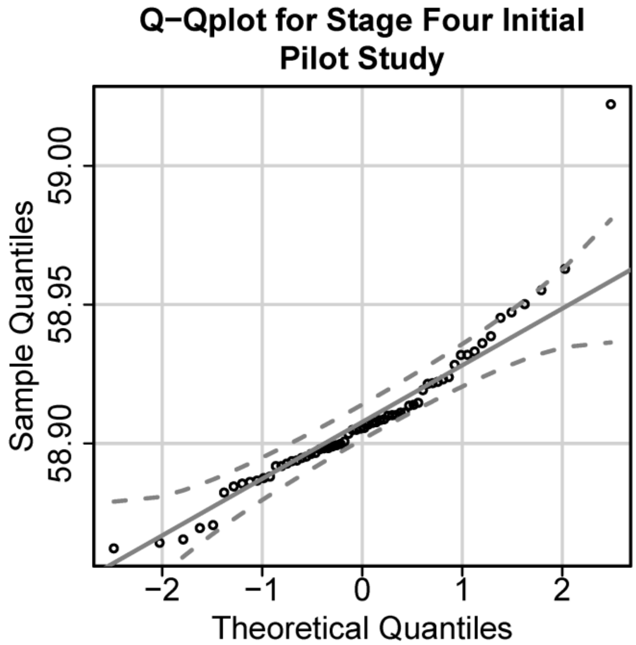

Figure 15. Pilot Simulation Q-Q Plot w/ 95% Confidence Interval for Stage Four (15% Communication Loss and 0 Untrusted Agents)

Because the goal of the SPS strategy is primarily to determine if the minimum frequency remains above 58.8 Hz, the outlier at a higher frequency does not negatively affect the stability of the power grid. A SPS control node quickly receiving enough updates to make a load shedding decision despite the communication delays and losses causes the outlier. Figure 16 and Figure 17 illustrate that when removing the outlier the data conforms to normal distribution. A Shapiro-Wilk normality test confirms the normal distribution with a p-value of 0.298 and a W value of 0.9774. [68] The null hypothesis for the Shapiro Wilk test is that the sample was drawn from a normally distributed population. The W value of 0.9774 is close to one and supports the null hypothesis. At the 95% confidence interval, the sample's p-value greater than 0.05 results in the overall acceptance of the null hypothesis.

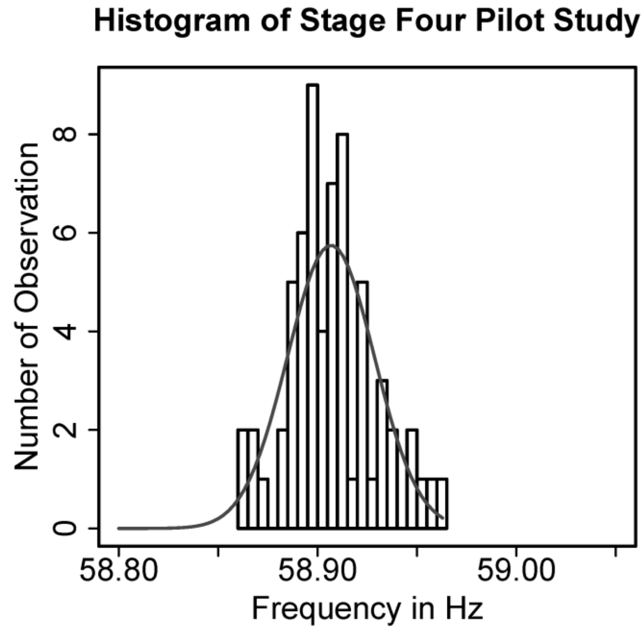

Figure 16. Revised Pilot Simulation Histogram for Stage Four (15% Communication Loss and 0 Untrusted Agents)

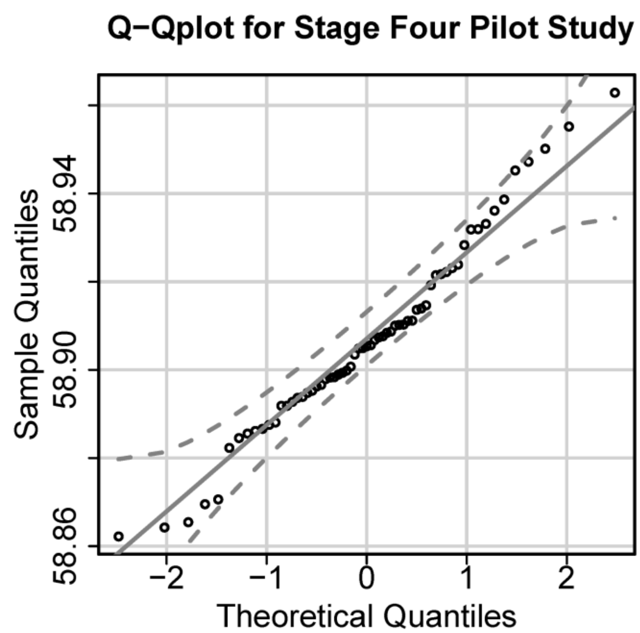

Figure 17. Revised Pilot Simulation Q-Q Plot w/ 95% Confidence Interval for Stage Four (15% Communication Loss and 0 Untrusted Agents)

Equation 6 is used to determine the minimum number of replications required to reach a 99% confidence interval for determining the mean of the simulation results. To compensate for deviation from normal and outliers the number of replications is tripled. The maximum error is determined from the pilot simulations. The mean frequency form the pilot simulation is 58.90854 Hz with a minimum frequency of 58.8622 Hz. The maximum error (E) = 0.02 is selected by using approximately one third the difference between the minimum frequency and the critical frequency (58.8 Hz). Additionally, the standard deviation for the pilot simulation is 0.02605121. The Z value used for 99% confidence interval is 2.58. Equation 6 determines the minimum number of replication is 12, and this research uses 36 replication. This results in 288 simulation trials for the main research. The research also includes several additional pilot simulations to provide the data utilized to make key design decisions such as the number of nodes to defend and to compare the strategic strategies to random strategies.

$$E = z\sigma_{\bar{x}} \rightarrow n = \frac{z^2\sigma^2}{E^2} \rightarrow 11.29367 = \frac{2.58^2 * 0.026051^2}{0.02^2} \tag{6}$$

4.7 Methodology Summary

This paper describes the research methodology used to evaluate a distributed decision making communication enabled SPS. The methodology defines and discusses the power transmission system and the distributed decision making SPS as the system and component under test. Additionally, the characteristics of the system are analyzed to determine the workloads, metrics, parameters and factors that affect the performance of the system. Simulation is selected as the appropriate evaluation technique and the experimental design required to achieve a 99% confidence interval is identified. This research methodology identifies a method to collect valid data required to evaluate and analyze the performance of the distributed decision making communication enabled special protection system.

V. Analysis and Results for Stages One-Three

5.1 Chapter Overview

This chapter presents results and analyses of experimental simulations from the evaluation of a distributed Special Protection Systems (SPSs) during the first three stages of the research. The results and analysis from the first stage of the research is presented and the results are compared to results from previous research concerned with applying trust to a centralized SPS. Next, results and analyses from the second stage of the research is presented and results are compared to results from previous research efforts concerned with overcoming communication delay and loss. This chapter will then present the results and analyses of the third stage of the research. Finally, the chapter will conclude with an overall analysis of the first three stages of the research.

5.2 Stage One: Distributed SPS with Simple Trust Management

This first set of experiments was conducted to assess the viability of an SPS using a distributed decision making approach. The experiments were based on Fadul's SPS research with modification to the behavior of the trust mechanism and a delay in the selection of an SPS load shedding strategy. Pilot simulations using Fadul's original trust mechanism occasionally produced false positives by indicating a trustworthy node was not trusted. These false positives typically occurred during a transient period such as immediately after generator 93 was removed from service.

Fadul's trust mechanisms operated without considering any historical data. The original trust mechanism evaluated trust using an instantaneous snapshot of the system taken every 2 milliseconds. The trust levels used to determine the SPS shed strategy were based upon the trust levels at the time the SPS determined the system needed load shedding for at least 8 milliseconds. The 8 milliseconds of detecting the requirement for load shedding prevented the system from shedding load due to the capture of a secondary transient event such as the opening or closing of a breaker for a transmission line.

The revised trust mechanism delays the trust decision 40 milliseconds to allow for the receipt of communication delayed updates and considers the trust updates received over the previous 42 ms (21 updates). Pilot simulations demonstrated that this approach's consideration of past trust values prevents false positive detection of trustworthy nodes. Additionally, pilot studies helped select 36 milliseconds of load shedding detection before determination of an SPS load shedding strategy for the distributed decision making SPS. This ensured missing data from communication delays and losses and secondary transient events do not trigger the determination and execution of an SPS load shedding strategy.

Fadul's SPS from previous research also utilized a different method for selecting nodes for load shedding. The process used in Fadul's SPS determined the minimum number of trusted nodes that could meet the load shedding requirements when shedding up to 20% of each individual trusted node. This typically resulted in 3-5 agents being selected to shed load. The load shedding process used by the revised distributed decision making SPS in the first stage of this research selects the largest 12 trusted nodes and divides the load shedding evenly between the 12 nodes.

5.2.1 Results and Analysis

The results of the first stage of the experiment demonstrated that the distributed decision making SPS maintained the system above the critical frequency of 58.8 Hz at all levels of adversarial disruptions. When compared to previous research, the revised distributed decision based SPS achieved similar performance in terms of successful operation of the SPSs when defending the system. When not defended, the revised distributed decision based SPS achieved a similar mean steady state frequency. However, the revised distributed load shedding process resulted in a significant increase in the standard deviation observed when the system was not defended. Figure 18 and Figure 19 show the results from the first stage of the research and the results from previous research. These figures illustrate that other than the difference in the standard deviation caused by the different load shedding processes, the distributed decision making SPS and the centralized decision making SPS from previous research produce similar results both when defending the SPS and when not defending the SPS. The distributed decision making SPS also sheds very little excess load indicated by the final frequency that is close to 58.8 Hz.

A visual analysis of Figure 18 indicates there is not a difference between the different levels of untrusted agents when the SPS defends the system. However, there appears to be a difference between the undefended and the defended results and there appears to be a difference between the undefended results at each level of untrusted agents. An ANOVA analysis between several means reinforces the visual analysis. The ANOVA test indicates indicating there is a significant difference in means with $p < 0.05$.

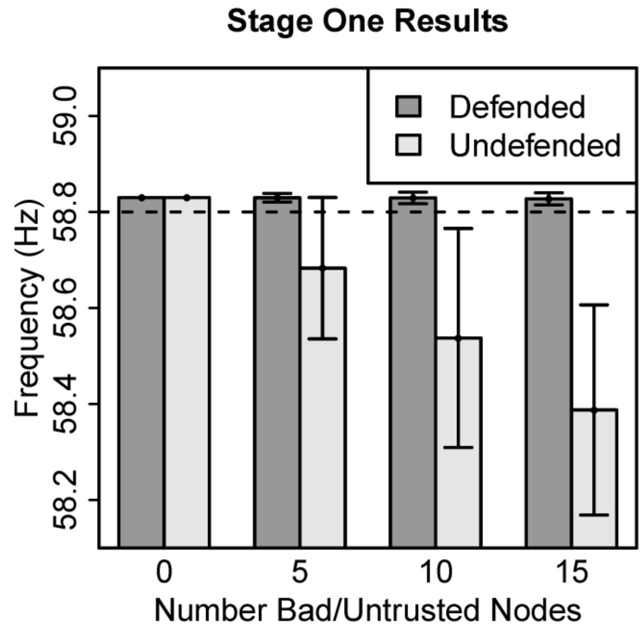

Figure 18. Stage One Results

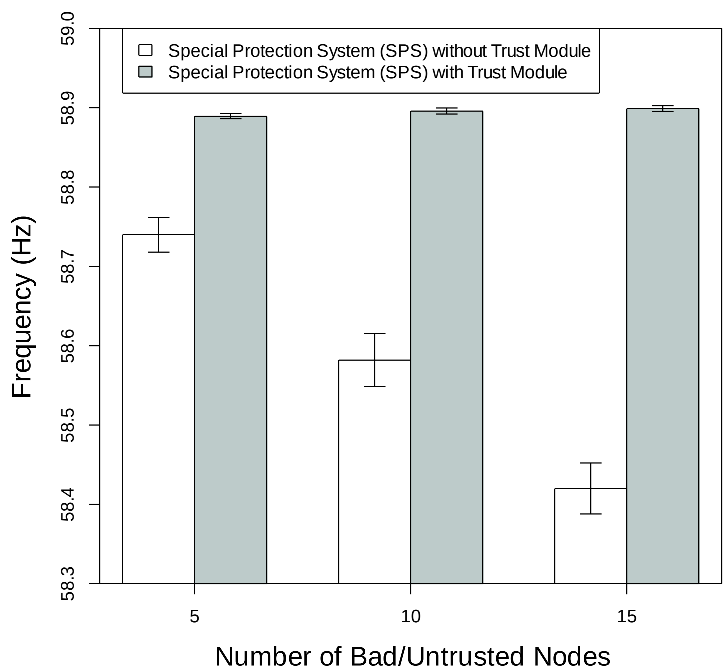

Figure 19. Previous Research Results [52]

5.2.2 Investigative Questions Answered

The analysis of the first stage of this research indicates that a distributed decision making communication enabled SPS using simple reputation based trust can successfully determine and execute an appropriate SPS load shedding strategy while experiencing various levels of disrupted agents. Additionally, the distributed decision making SPS performs similarly to the centralized decision making SPS from previous research.

5.3 Stage Two: Distribute SPS with Background Traffic and Communication Loss Mechanism

The second set of experiments was conducted to test the data retransmission scheme developed to mitigate data loss due to background traffic and cyber-attacks that disrupt communications. In this scheme, load and generator agents push one update every 2 ms and push the last 30 updates every 6 ms. This allows the SPS decision agents to reconstruct past system states that were not updated due to communication losses. This stage of the research focused on just the communication loss and does not include attacks to disrupt individual agents. Additionally, as the amount of time between the rejection of generator 93 and the determination of a load shedding strategy increases, the system generators continue to slow down, losing intertia. The loss of inertia requires more capacity to be shed in order to maintain system stability. For this reason, the formula to determine the amount of load that must be shed is adjusted to compensate for the delays caused by communication losses.

5.3.1 Results and Analysis

The results of the second set of experiments indicates the distributed decision making SPS using a retranmission scheme to overcome communication disruptions successfully maintains the system above the critical frequency at all levels of communication disruption. Additionaly, the results indicate that the standard deviation grows as the amount of disruption increases. The growing standard deviation is a result of the variation in the amount of time required for the SPS to reconstruct the system state due to communication losses. ANOVA analysis indicates there is a statistical difference between the system operating with no communcation disruption and the system operating with all three levels of disruptions ($p < 0.05$). ANOVA analysis also indicates there is no statistical difference between 5% and 10% communication disruption or between 5% and 15% communication disruption ($p > 0.05$), however the difference between 10% and 15% communication disruption is statistically significant ($p < 0.05$). This anomoulous conclusion results from the difference in the standard deviation observed at each level of disruption. The difference in the system response indicates the communication disruption changes the response of the system. However, the levels of communication loss evaluated by the experiments in this stage of the research do not prevent the successful operation of the SPS.

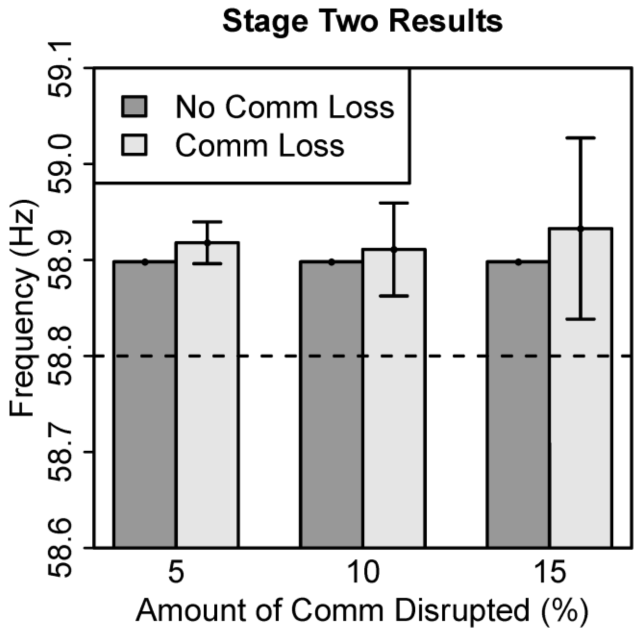

Figure 20. Stage Two Results (Communication Disruption)

5.3.2 Investigative Questions Answered

A distributed decision making communication enabled SPS using simple reputation based trust can successfully determine and execute an appropriate SPS load shedding strategy while experiencing various levels of network traffic and losses. The analysis of the second stage of this research indicates that the retransmission scheme used in this distributed decision making SPS successfully overcomes the delays and losses caused by background traffic and up to 15% communication loss due to disruptions caused by malfunctions or cyber-attacks.

5.4 Stage Three: Distributed SPS with Background Traffic, Communication Loss and Revised Trust Management Mechanism

The third stage of this research tests the distributed decision making SPS while operating with both disruptions to individual agents and disruptions in communication. In this stage, the SPS uses the reputation based trust mechanisms to detect malfunctioning or disrupted load agents and overcomes communication delays in order to determine and execute the load shedding strategy.

5.4.1 Results and Analysis

The results from the third stage of this research indicate the distributed decision making SPS successfully maintains the system above the critical frequency at all evaluated combinations of communication disruption and disruption of nodes. ANOVA analysis indicates there is a significant difference between the system response when utilizing the trust based mechanisms to protect the system and when not using the trust based protection mechanisms ($p < 0.05$). ANOVA analysis indicates there is no significant difference in the system response when using both the trust mechanisms and the retransmission scheme when faced with the combination of communication and agent disruptions evaluated in this stage of the research ($p > 0.05$).

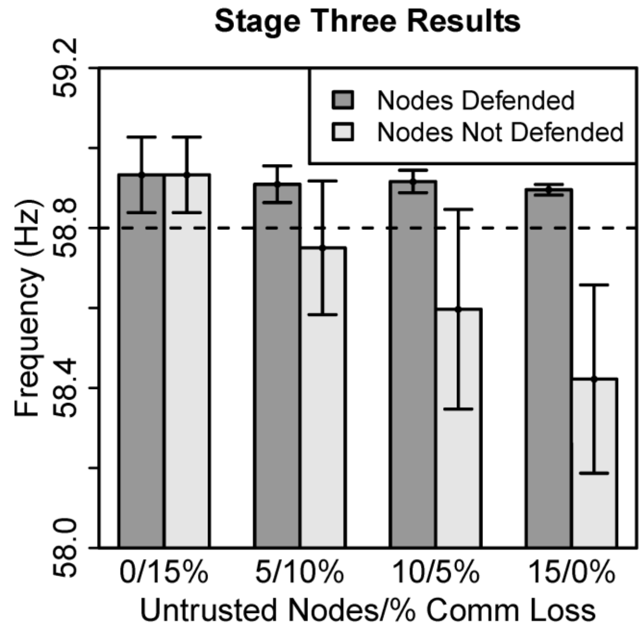

Figure 21. Stage Three Results (Bad Nodes and Communication Losses)

In addition to the final experimental results, the operation of the trust mechanism is illustrated and analyzed. Figure 22 shows the initial instantaneous trust values determined by the SPS trust mechanism and Figure 23 shows the average initial trust values for the trusted and untrusted nodes. These trust determination are based upon the most recent observations used to determine the overall trust for each node. The initial trust determinations are delay 40 ms to allow the control agents to reconstruct the system state from data received by the retransmission mechanism. This figure shows that the trusted nodes, nodes 25, 34, 35, 59, 64, 65, 67, 70, 71, 72, 73, 78, 85, 88, 133 and 138, maintained trust above 85 while the untrusted nodes, nodes 14, 27, 51, 58, 63, 66, 69, 74, 75, 81, 83, 84, 86 and 120, maintained trust below 85. Similar to the initial values, Figure 24 shows an intermediate instantaneous trust value determined by the trust mechanism and Figure 25 shows the average trusted and untrusted nodes. Theses intermediate trust value determinations are delayed 60 ms. This delay results in additional reconstruction of past system states increasing the number of nodes strongly trusted or untrusted. Finally, Figure 26 shows the final trust values used by the system. The final trust values are determined using instantaneous trust values averaged over a 40 ms period. The 40 ms period used to determine the final trust values begins at 40 ms in the past and ends to 80 ms in the past. Figure 27 shows the average of the final trust values for the trusted and untrusted nodes. By using trust values determined using 40 ms of history, the trust mechanism prevents false positive and false negative trust determinations due to shorter term transient responses.

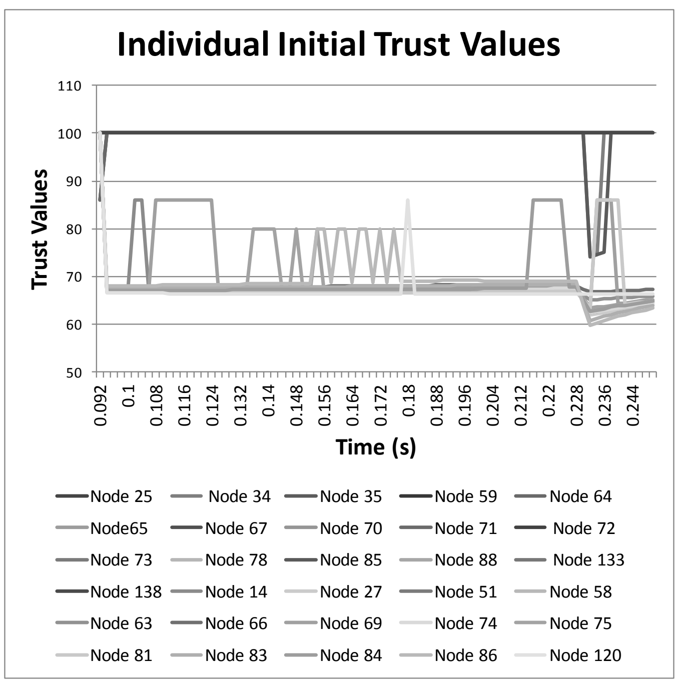

Figure 22. Individual Initial Instantaneous Trust Values

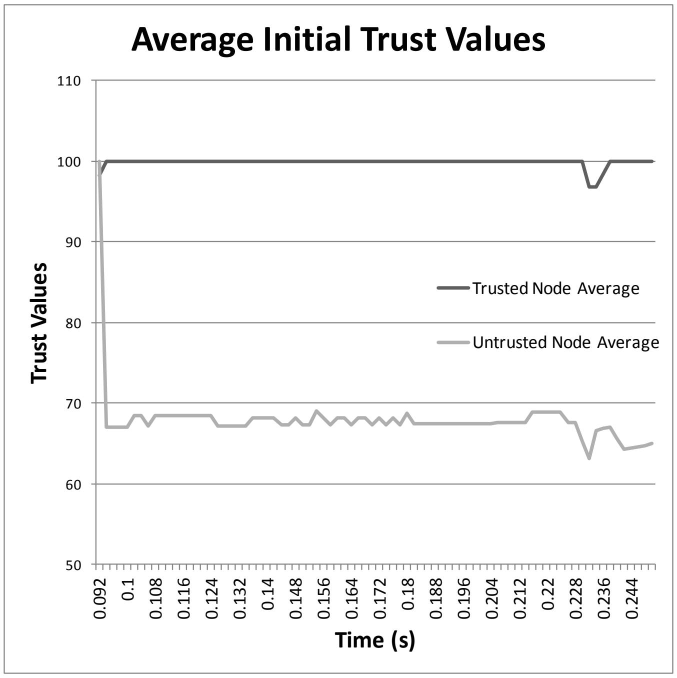

Figure 23. Average Initial Instantaneous Trust Values

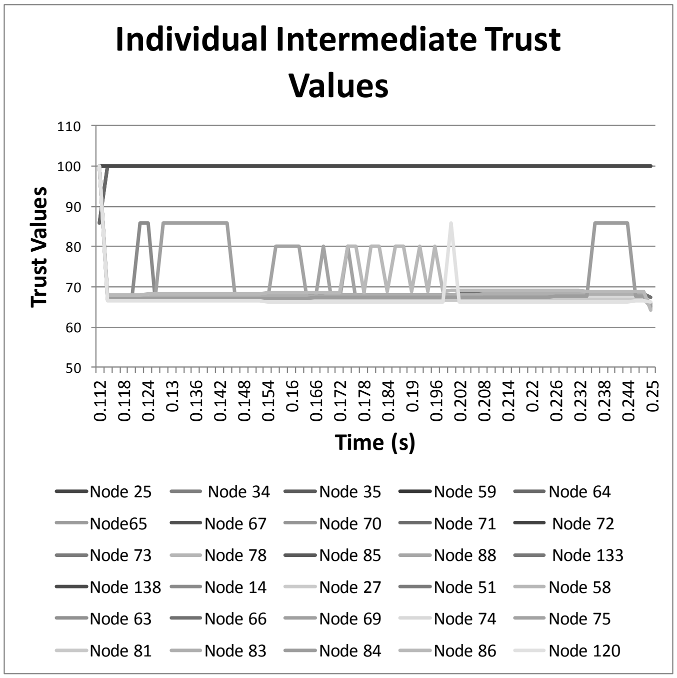

Figure 24. Individual Intermediate Instantaneous Trust Values

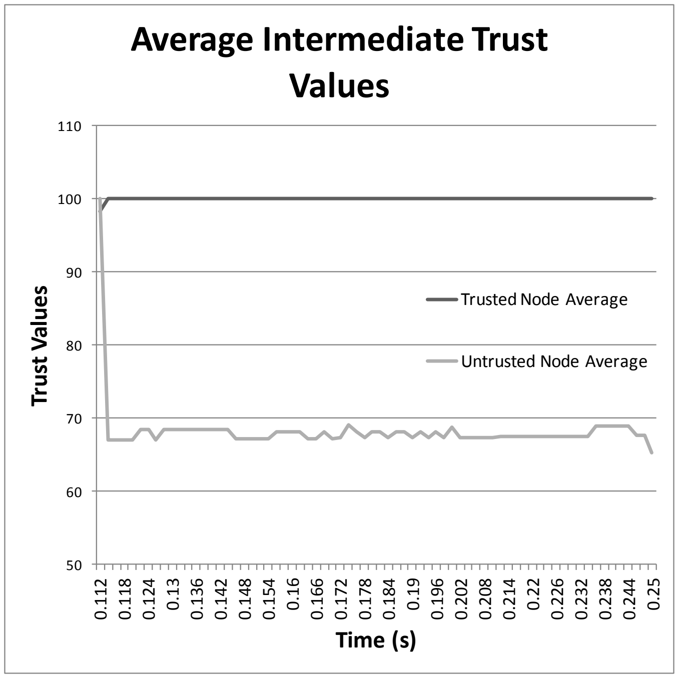

Figure 25. Average Intermediate Instantaneous Trust Values

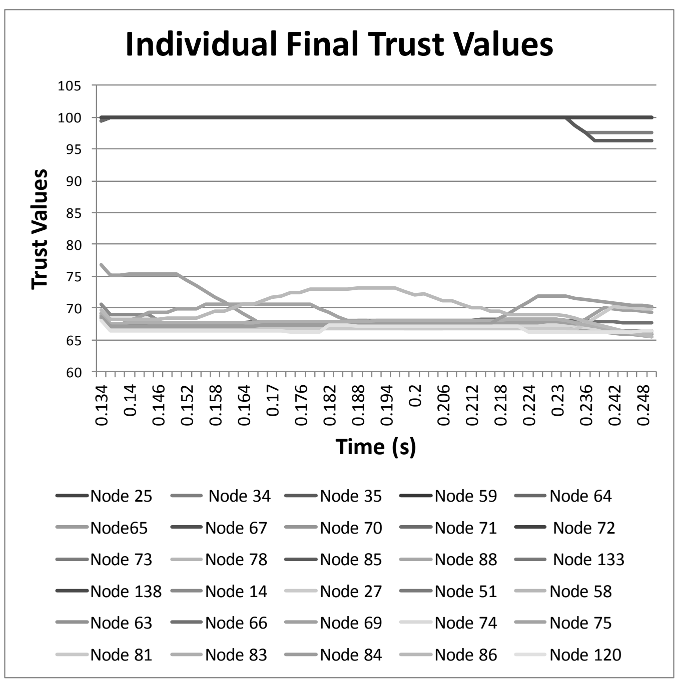

Figure 26. Individual Final Trust Values

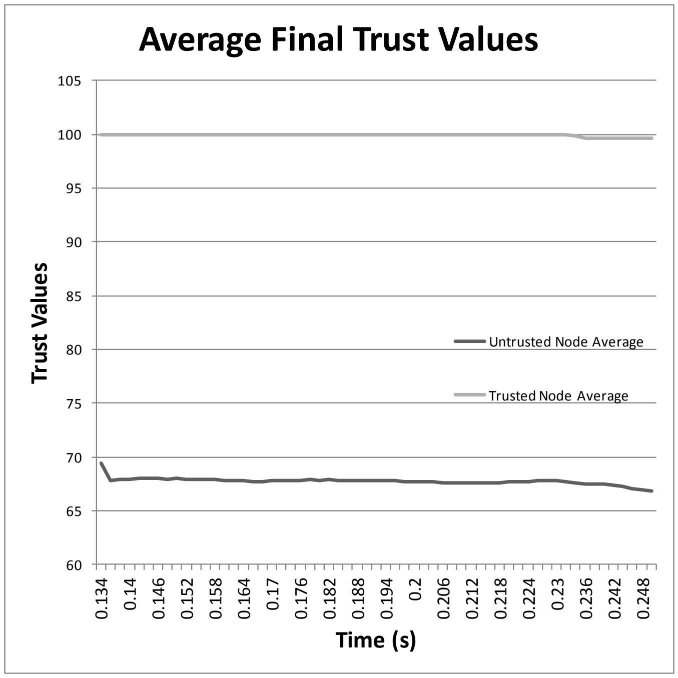

Figure 27. Average Final Trust Values

5.4.2 Investigative Questions Answered

A distributed decision making communication enabled SPS using simple reputation based trust can successfully determine and execute an appropriate SPS load shedding strategy while experiencing various levels of network traffic and losses and various levels of disrupted agents. The analysis of the second stage of this research indicates that the reputation based trust mechanism and communication retransmission scheme used in this distributed decision making SPS successfully maintains the system above the critical frequency when operating with a combination of up to 15 disrupted nodes and up to 15% communication losses with background traffic.

5.5 Summary of Stages One-Three

The first three stages of this research provided the testing and evaluation to validate the development of a communication enabled distributed decision making SPS using reputation based trust to protect an SPS load shedding process from malfunctions and cyber-attacks. The first two stages of the research evaluated revised mechanisms for overcoming malfunctioning or disrupted nodes and communication disruptions due to background traffic and cyber-attacks. The third stage evaluated the combination of the new mechanisms from the first two stages of the research and validated the SPS's response when reacting to malfunctioning or disrupted nodes and to communication losses at the same time. Additionally, the first three stages of the research demonstrated that an SPS load shedding scheme can determine and execute a load shedding strategy using a distributed process rather than a centralized process removing a possible single point of failure. Finally, the first three stages of the research validated the development of a communication enabled distributed decision making SPS using reputation based trust that could be adapted to use a game theoretic approach to reduce the cost of defending the SPS from malfunctions and cyber-attacks.

VI. Analysis and Results for Stage Four

6.1 Chapter Overview

This chapter presents results and analyses of experimental simulations from the evaluation of a distributed Special Protection Systems (SPS) utilizing a game theoretic approach to strategically defend the SPS's load shedding process. In this stage of the research, the SPS is cost constrained preventing the monitoring and defense of every node. Additionally, the cost constrained adversary also utilizes strategy to maximize the probability of disrupting the SPS load shedding process. In addition to the primary results from the optimized SPS and adversarial strategies, pilot studies that guided design decisions and the results from alternative SPS and adversarial strategies are presented to demonstrate the development of the game theoretic approach and properties of the game theoretic approach. Additionally, the performance of the SPS when facing the random adversarial strategy from the third stage of the research is compared to the performance of the optimized adversarial strategy from this stage of the research. Finally, the chapter will conclude with an overall analysis of this stage of the research.

6.2 Results and Analysis

After analytically developing an optimal monitoring and protection strategy and the optimal adversarial node disruption strategy, the first stage of this research involved running pilot studies to validate the strategy. The initial pilot studies evaluated the SPS load shedding strategy when defending different numbers of nodes. Initial pilot studies reinforced the conclusion that the SPS must defend 22 nodes to ensure a greater than 98%

probability of successful load shedding actions given the 90% probability of detecting the nodes disrupted by the adversary's attack strategy. Figure 28 shows the results from the first round of pilot studies and demonstrates that the SPS successfully protected the load shedding process when defending 22 nodes by keeping the system frequency above 58.8 Hz. However, additional refinements in the process of selecting the trusted load nodes reduced the number of nodes required to provide a 98% probability of success to 21. Figure 29 shows the results from the second round of pilot studies where the SPS successfully protected the load shedding process when defending 21 nodes by keeping the system frequency above 58.8 Hz. The remainder of the research continued with an SPS monitoring and protection strategy defending 22 Nodes.

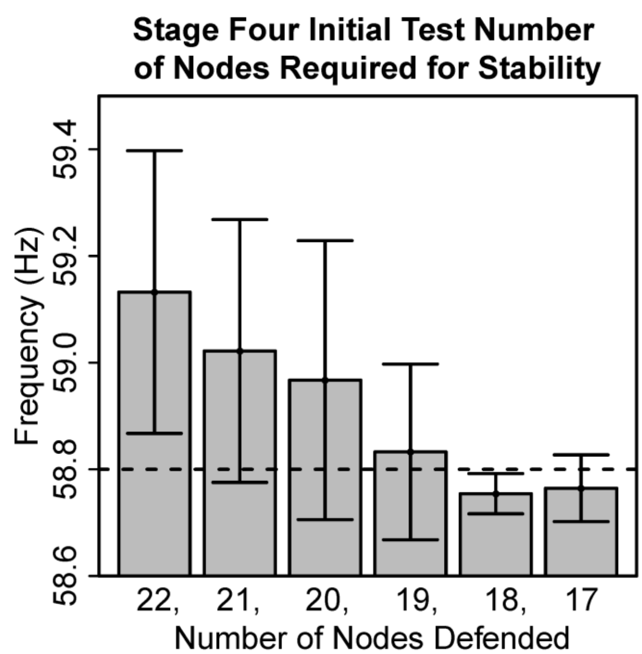

Figure 28. Stage Four Initial Pilot Study to Reinforce the Analytical Determination of the Minimum Number of Agents Required to Defend the SPS Load Shedding Process

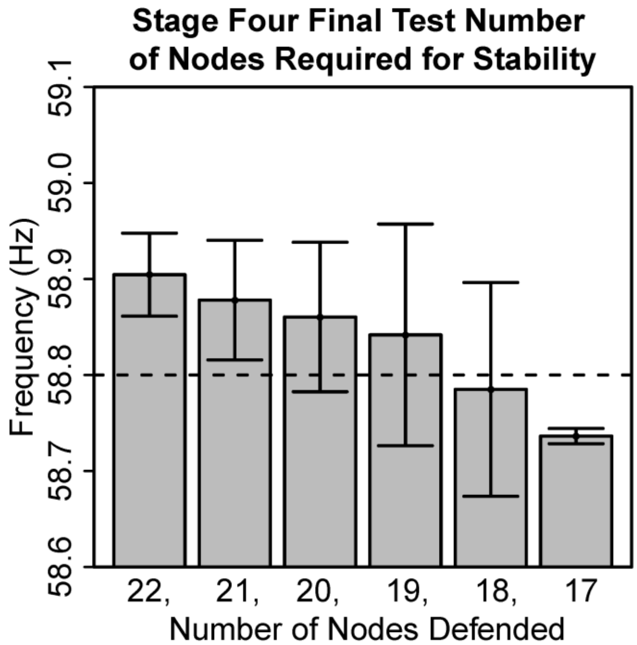

Figure 29. Stage Four Revised Pilot Study to Reinforce the Analytical Determination of the Minimum Number of Agents Required to Defend the SPS Load Shedding Process

After validating the number of nodes that the SPS must defend, the examination of the SPS continued with the primary experiment for this stage of the research. The primary research evaluated the communication enabled distributed decision making SPS using reputation based trust and game theory to defend the SPS load shedding strategy while an adversary attacks the system by disrupting a proportional combination of up to 15 nodes and up to 15% of the communication. Figure 30 shows the results from this stage of the research's primary experiment. The SPS in this stage of the research successfully defended the SPS load shedding process by keeping the frequency above 58.8 Hz when operating against each level of the adversary's disruption. Additionally, there appears to be a statistically significant difference in the results when defending the SPS load shedding process and when not defending the SPS load shedding process from malfunctioning or disrupted nodes. An ANOVA analysis of the experimental results reinforces the conclusion that there is a statistically significant difference between the defend and undefended SPS load-shedding process ($p < 0.05$).

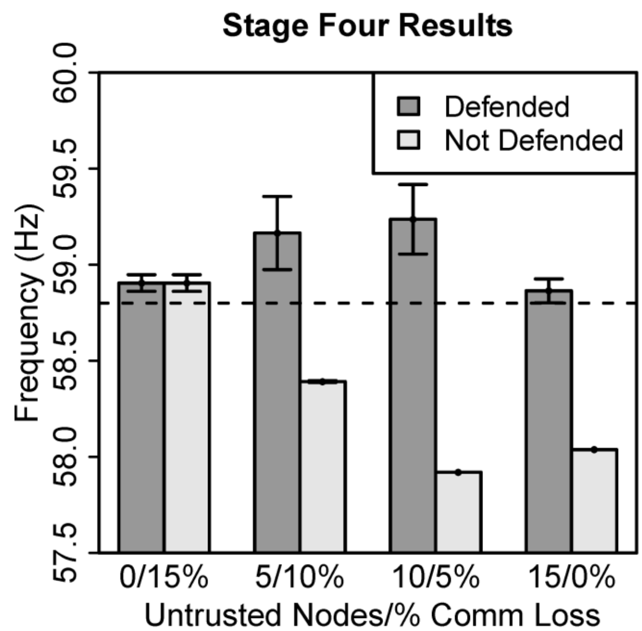

Figure 30. Primary Results for Stage Four of the Research

In addition to the experiments to determine the success or failure of the SPS, further experiments highlight the game theoretic properties of the SPS and adversary. A premise of the strategy used for the defense of the load shedding process is that the strategy is an optimal strategy. More specifically, the strategy is a dominate strategy and also produces a Nash Equilibrium when the adversary employs an optimal strategy. To be a weakly dominate strategy; the strategy must result in a equal or better utility compared to other possible strategies. To be a Nash Equilibrium neither strategy benefits from changing unilaterally.

Figure 31 and Figure 33 demonstrate the SPS's strategy as a weakly dominate strategy. Figure 31 shows that the optimal strategy produces a higher utility by maintaining the critical frequency above 58.8 Hz for all combinations of the adversary's optimal attack and the bad defensive strategy results in the failure to maintain the critical frequency above 58.8 Hz during attacks on ten or 15 nodes with no statistical difference in the final frequency when five nodes are attacked. Figure 33 illustrates that compared to the optimal defensive strategy, a random SPS defense maintains the critical frequency above 58.8 Hz when the adversary attacks five or ten nodes with no statistical difference, however the random strategy results in a statistically significant excess amount of load shedding during attacks on 15 nodes. The analysis of the figures is reinforced by ANOVA analysis with ($p < 0.05$) for results that are statistically different and ($p > 0.05$) for results that are statistically the same.

The game formulation used to model this system is not a zero sum game. The utility for the adversary is not directly related to the utility for the SPS. In this game formulation the adversary is not fully aware of how many nodes are protected by the SPS monitoring strategy. The optimal offensive strategy is also a weakly dominate strategy. The adversary achieves the greatest utility by maximizing the probability that the frequency will drop below 58.8 Hz. Figure 32 illustrates how the adversary achieves the greatest probability of causing the frequency to drop below 58.8 Hz when using an optimal strategy when attacking 10 or 15 nodes. The results when optimally attacking 5 nodes is statistically different than when attacking with a bad offense, however the results do not indicate a higher probability of dropping the frequency below 58.8 Hz. The analysis of the figures is reinforced by ANOVA analysis with ($p < 0.05$) for results that are statistically different and ($p > 0.05$) for results that are statistically the same.

Analysis of Figure 31, Figure 32, Figure 33 and Figure 26 supports the premise that the optimal defensive and adversarial strategies are at a Nash Equilibrium. When the adversary's strategy changes from optimal and the SPSs defensive strategy remains optimal, the adversary achieves less utility. Additionally, when the SPS changes the defensive strategy from optimal and the adversary's strategy remains optimal the SPS achieves less utility. Figure 31 and Figure 33 demonstrate that the optimal defense strategy performs better than, or equal to, both the bad and random defensive strategies and there is no incentive for the SPS to unilaterally change from the optimal strategy to another strategy. ANOVA analysis provides support for this observation by indicating a ($p < 0.05$) statistically significant difference in between the performance of the optimal and bad defense when 10 and 15 nodes are attacked and between the performance of the optimal and random defense when 15 nodes are attacked. All of the other levels of attack produce statistically similar results with ($p > 0.05$). Figure 32 and Figure 34 demonstrate that the optimal offensive strategy performs better than, or equal to, both the bad and the random offensive strategies and there is no incentive for the adversary to unilaterally change from the optimal strategy to another strategy. ANOVA analysis provides support for this observation by indicating a ($p < 0.05$) statistically significant difference between the performance of the optimal and bad offense when 10 and 15 nodes are attacked and between the performance of the optimal and random defense when 15 nodes are attacked. All of the other levels of attack produce statistically similar results with ($p > 0.05$).

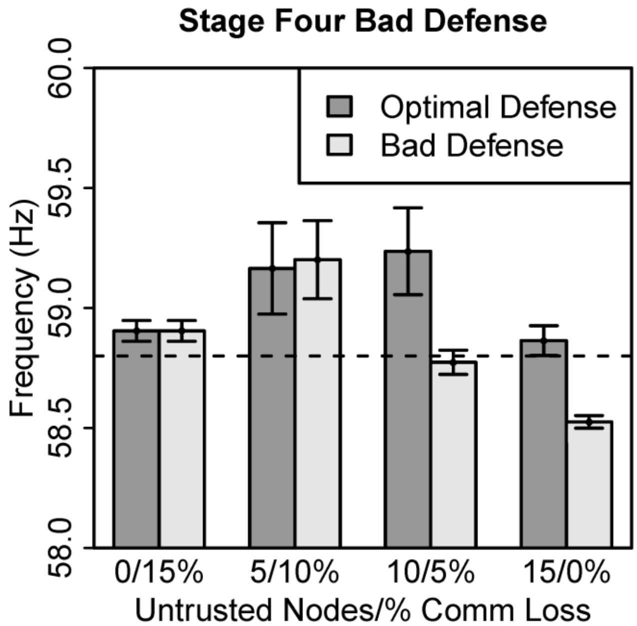

Figure 31. Stage Four Bad Defensive Strategy vs. Optimal Adversarial Strategy Results

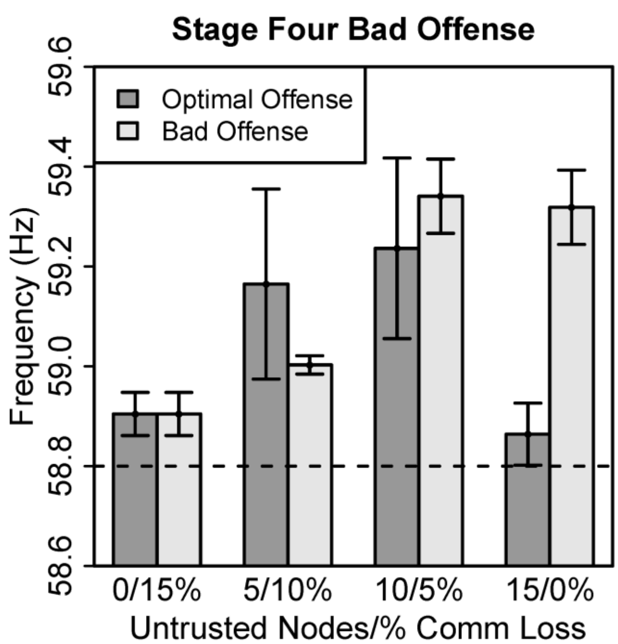

Figure 32. Stage Four Bad Adversarial Strategy vs. Optimal Defensive Strategy

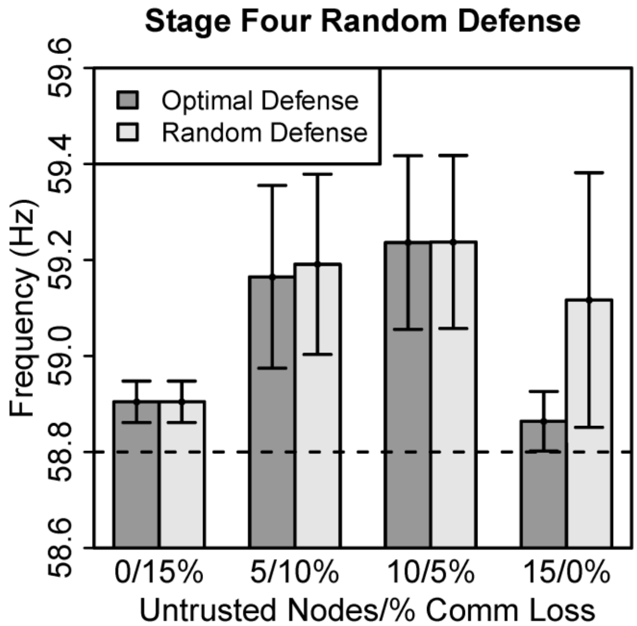

Figure 33. Stage Four Optimal Adversarial Strategy vs. Random Defensive Strategy

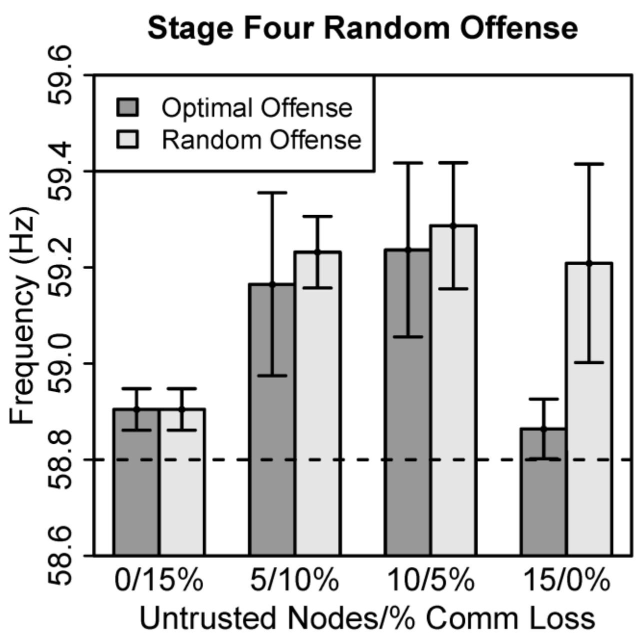

Figure 34. Stage Four Optimal Adversary vs. Random Defensive Strategy

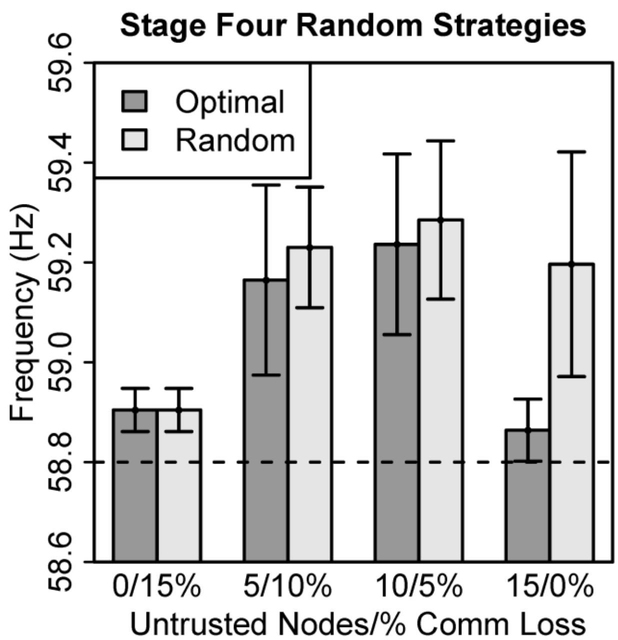

Figure 35. Stage Four Random Adversarial Strategy vs. Random Defensive Strategy

Additional experiments tested the performance of the optimal game theoretic attack strategy against the defense strategy used in the third stage of the research while constraining the SPS monitoring to a 90% probability of detecting the disrupted SPS node. Differences in the performance illustrate the contributions of the game theoretic approach used to defend the SPS load shedding process. Figure 36 demonstrates that there is a statistically significant difference in the results when comparing the defensive strategy from stage four to the defensive strategy used in stage three of this research. The defensive strategy used in stage three fails to maintain the minimum observed frequency above 58.8 Hz at all levels of attack with a significantly poorer performance when 15 nodes are attacked. Observations are reinforced by ANOVA analysis with a ($p < 0.05$) for all statistically different observations.

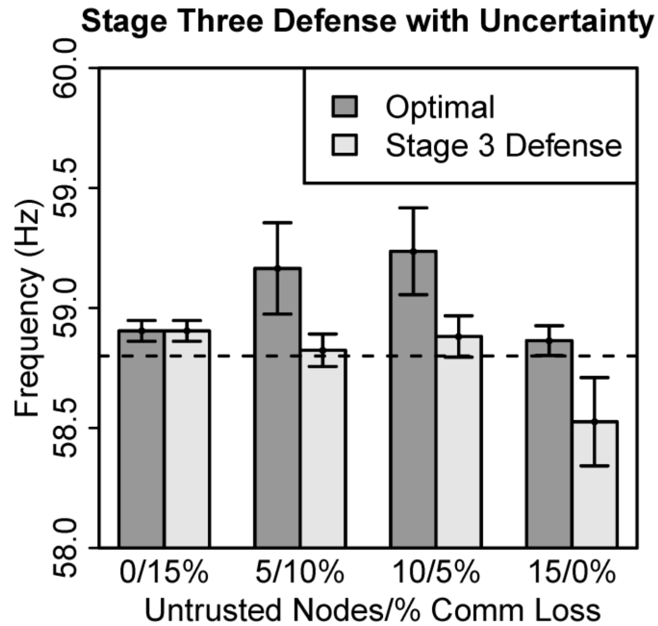

Figure 36. Stage Four's Optimal Adversarial Strategy vs. Stage Three's Defensive Strategy

A final set of experiments tested the performance of further resource constrained SPSs against an adversary with a random attack against 15 nodes. Figure 37 demonstrates that when monitoring only 16 nodes, the SPS load shedding strategy remains successful against a random adversary with a 90% probability of detection. When the SPS defended nine nodes, the SPS successful shed the required load 47.2% of the time. Additionally, the strategic approach for defending 10 nodes performed equivalently to the non-strategic approach defending all 30 nodes against a random adversary with a 90% probability of detection. ANOVA analysis confirms that the resource constrained SPS using an optimal strategy performs statistically the same ($p > 0.05$) as the non-strategic strategy defending all 30 nodes. This result shows the strength of the stochastic decision process that is part of the game theoretic approach for defending the SPS.

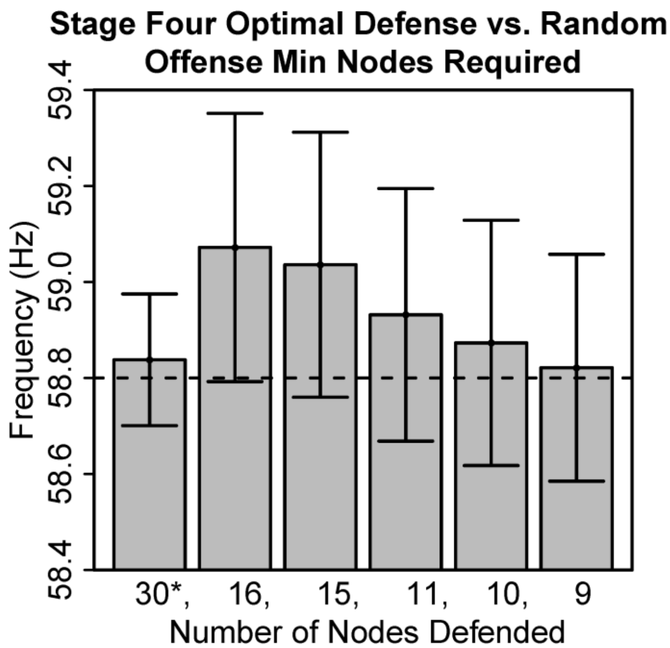

Figure 37. Stage Four Test to Determine Effects of Additional Resource Constraints on the SPS strategy vs. a Random Adversary

6.3 Investigative Question Answered

This research demonstrates that a distributed decision making communication enabled SPS using a resource constrained simple reputation based trust mechanisms can use game theory principles to successfully determine and execute an appropriate SPS load shedding strategy while experiencing various levels of network traffic and losses and various levels of disrupted agents introduced by a resource constrained adversary also using a strategy determined from game theory principles. Additionally, this stage of the research demonstrates that a strategic relationship between a communication enabled distributed decision making SPS and an adversary attempting to disrupt the execution of the SPS can be modeled and analyzed using game theoretic principles.

6.4 Summary of Stage Four

The final stage of this research provided results from the testing and evaluation used to validate the development of a communication enabled distributed decision making SPS using reputation based trust and game theory to protect an SPS load shedding process from malfunctions and cyber-attacks. This stage of the research analyzed the use of game theoretic principles to determine an optimal SPS protection strategy and an optimal attack strategy given resource constraints. The research continued by examining the test results from various alternative strategies to demonstrate the optimality of the primary SPS protection and attack strategies and to demonstrate the game theoretic properties of the strategy. The results from this stage of the research demonstrate the success of the game theoretic approach for defending the SPS load shedding process against adversarial actions.

VII. Conclusions and Recommendations

7.1 Chapter Overview

This chapter reviews the high level goals and results from this research effort to develop and test a new approach to performing SPS load shedding actions using a distributed decision making procedure and the application of game theory to optimize the protections of the SPS load shedding process. The chapter continues by addressing the significance of this research and makes recommendations for action. Finally, this chapter suggests areas for future research to further validate the results observed and provides additional areas to further improve and refine this approach to defending an SPS load shedding process.

7.2 Conclusions of Research

This research demonstrates that an SPS load shedding strategy can be done in a distributed manner. Additionally, the results demonstrates that simple reputation based trust and retransmission mechanisms can overcome detectable and partially detectable attacks against a communication enabled distribute decision making SPS. Finally, this research demonstrates that game theory can be used to model and analyze the strategic relationship between resource constrained monitoring and defense strategies and a resource constrained adversary.

7.3 Significance of Research

While the results of this research demonstrate the success of this significant departure from traditional SPSs, the research is an observational study. This research determined that the distributed decision making approach and use of game theory to performing SPS load shedding action works in this specific scenario and warrants further investigation to determine applicability to other scenarios. Aspects of this experiment are randomized. However, there is only one scenario evaluated, and only one solution evaluated. No inference to other scenarios or other solutions can be made from this research.

7.4 Recommendations for Action

This research suggests that further development and testing of distributed processes and the application of game theory to model strategic relationships can strengthen the defense of the smart grid and other SCADA systems. The outcome of this research should motivate further development and testing to validate the results observed in this research. If further development and testing reinforces the results from this research and demonstrates the applicability to a wider range of power disturbance scenarios, the use of distributed control process and game theory should be integrated into future smart grid designs.

7.5 Recommendations for Future Research

This research represents a significant departure from traditional SPSs, recently researched SPSs and control mechanisms in current SCADA systems. Additionally, the demonstrated success of this research generates a significant number of recommendations for future research. Suggested areas for further research:

1. Test this distributed control approach and game theoretic model with more realistic abuse cases requiring more sophisticated trust and or detection mechanisms.
2. Evaluate additional SPS load shedding scenarios added to this power grid model to determine the response to multiple possible disruptions requiring different amounts of load shedding.
3. Adapt and test this SPS load shedding methodology with other equally or more sophisticated power grid models to further examine the application of the distributed decision making process and game theory to improve the protection of SPSs and other smart grid functions.
4. Analyze the power grid and communications network to optimize the number and location of the SPS control nodes and compare the results to this and previous research.
5. Adapt and evaluate system state estimation mechanisms from past research to overcome greater amounts of communication losses and delays.
6. Adapt this decentralized process to a more traditional agent based peer-to-peer network architecture with each SPS control node receiving updates from specific load and generator nodes and requiring the SPS control nodes to develop a load shedding strategy cooperatively rather than independently as is done in this research.

7.6 Summary

In an effort to improve the security and protection of United States' critical infrastructure, this research investigates a new approach to help secure and protect the SPS load shedding strategy that is an integral part of the modern power grid. The research introduces many concepts and fundamental properties of SCADA systems, the future smart gird, SPSs, trust systems, game theory and previous research efforts to develop and protect a communication enabled SPS. Next, this thesis details the methodology used to evaluate the four stages of this research. The results from the research methodology demonstrates the successful development of a communication enabled distributed decision making SPS using simple reputation based trust and game theory to overcome cyber-attacks against the power grid. Finally, this research concludes with recommendations for action and future research.

Appendix A. SPS Game Theory Formulation

The game in this research is a hybrid, single, simultaneous, asymmetric, non-zero sum game with incomplete knowledge. The SPS players are assumed to have some limited communication capability so that the execution of the strategy is coordinated. However, there is no mechanism to enforce cooperation; the strategies selected by each SPS are based upon beliefs about the state of the game and the assumed rational actions of the adversary. The adversary in this research is modeled as a single player; no coalition or coordination is required. The game is a one-time game where each player selects an action without knowing the actions selected by the other players. The utility and cost functions for the players do not sum to zero or any other constant and are not symmetric. Finally, the game is Bayesian in nature. The SPS is not fully aware of all the strategies available to the adversary and the adversary is not fully aware of all the strategies available to the SPS. Players make assumptions and use probabilities derived from limited observations and beliefs about rational behavior to select defense and attack strategies.

The game played by the SPS and the adversary is the first step in the process of determining an SPS load shedding strategy. The SPS does not know how many nodes or how much communication the adversary can disrupt as part of an attack strategy, but can make predictions about the performance of possible strategies. From the SPS's perspective, the goal of the game is to reduce the level of uncertainty in the system state so that a load shedding decision can be made that takes uncertainty into consideration. Once the SPS executes its strategy, the SPS uses systems observations to form beliefs about the game state. From the beliefs, the SPS makes a load shedding decision that considers the stochastic nature of the system state. The SPS optimizes the defense strategy for maximum effectiveness against the possible adversary attack strategies believing that there are constraints that prevent the attack of more than 15 nodes.

From the adversary's perspective, the goal is to disrupt the SPS load shedding decision process so that the SPS fails to maintain system stability after a disturbance by strategically disrupting load nodes and/or disrupting communication. The adversary does not know how many nodes are protected by the SPS, but can predict the performance of possible SPS protection strategies. The adversary optimizes the attack strategy for maximum effectiveness against the possible SPS defensive strategies believing that there are resource constraints that prevent the protection of every node.

In the execution of the SPS actions, the SPS decision agents make assumptions about the system state based formed from observations and beliefs about the adversary. Specifically, the SPS decision agents assume the adversary can disrupt a combination of up to 15 agents or 15% of the communication, and that the SPS detects disrupted agents with a 90% normally distributed probability. SPS decision agents use predictions based on the number of disrupted agents detected to determine a load shedding strategy. The SPS decision agents compensate for possible undetected disrupted agents and adjust the load shedding strategy to ensure system stability with a minimum of 98% probability of success. Further, the SPS load shedding strategy also attempts to minimize the amount of excess load shedding after guaranteeing a 98% probability of success. Ensuring the required probability of successful load shedding actions requires the selection of enough excess load to negate the number of bad nodes that may receive shed commands. Although a higher level of probability for success is desirable, analysis of the game environment during pilot studies revealed that higher levels of probability significantly increase the number of loads and the amount of power that must be shed.

In terms of utilities, the SPS gains maximum utility by ensuring the frequency remains above 58.8 Hz. The adversary gains maximum utility by causing the frequency to drop below 58.8 Hz. The adversary gains a smaller amount of utility by causing excess load shedding. Costs for the SPS include the expense of defending each agent and the expense related to shedding excess load. Costs for the adversary include the expense of attacking each agent and the costs related to attribution. The maximum cost for the adversary is limited by assumptions about the rationality and capability of an adversary. A secondary justification for the limitations is that pilot simulations and analytical evaluation of the game demonstrated that an unconstrained adversary is unbeatable. The maximum costs for the SPS is limited by the assumption that the power grid operator will desire to maximize profit by minimizing expenses.

$$G = \langle N, A, U \rangle \tag{7}$$

$$G = \langle \{n_{sps\ 1\ldots n}, n_{adv}\}, \{a_{sps\ 1\ldots n}, a_{adv}\}, \{u_{sps\ 1\ldots n}, u_{adv}\} \rangle \tag{8}$$

$$n_{sps\ 1\ldots n} = \{SPS\ control\ nodes\}$$

$$n_{adv} = \{Adversary\}$$

$$a_{sps\ 1\ldots n} = \{Each\ SPS\ Control\ Node\ Selects\ 22\ Nodes\ from\ 30\ Nodes\ to\ Defend$$

$$a_{adv} = \{Proportionaly\ select\ up\ to\ 15\ Nodes\ from\ 30\ Load\ Nodes$$

$$to\ disrupt\ or\ 15\%\ Comm\ Disruption\}$$

$$u_{sps} = \{1{,}000{,}000 * p_{success} - 1{,}000{,}000 * p_{failure} - ((100{,}000 * (final\ freq - 58.8))\ \ if\ final\ freq > 58.8\ ) - (10000 * Nodes\ Monitored)$$

$$u_{adv} = \{1{,}000{,}000 * p_{success} - (100{,}000 * (Nodes\ Attacked\ or\ Comm\ Disrupted) * p_{attribution}) + (1{,}000 * (final\ freq - 58.8))$$

G – Game Components

N – Set of Players

A – Action Space

U – Set of Utility Functions

n_{sps} – SPS Players (each operates independently, but with the same strategy)

n_{adv} – Adversary Player

a_{sps} – Set of Actions Available to SPS

a_{adv} – Set of Actions Available to Adversary

u_{sps} – SPS Utility Function

u_{adv} – Adversary Utility Function

$p_{success}$ – Probability of Success

$p_{failure}$ – Probability of Failure

$p_{attribution}$ – Probability of Failure Being Attributed to Adversary

In this game formulation, the actions that the SPS and the adversary select determines the probability of success and failure as well as the probability of the attack being attributed to the adversary. As revealed in Chapter 4, the SPS has 5,852,925 possible strategies from which to select and the adversary has a different number of strategies from which to choose based on the number of nodes selected for attack. When selecting to attack 15 nodes, the adversary has 155,117,520 possible strategies, 30,045,520 possible strategies when attacking 10 nodes, and 142,506 possible strategies when attacking 5 nodes. At the three levels of attack evaluated in this research there are 1.08458e+15 possible combinations of strategies. However, analysis of the game space reveals dominate strategies for both the SPS and the adversary.

At the simplest level, the goal of the SPS is to develop trust over enough nodes so that even with the uncertainty left by the 90% detection rate for the adversary's attacks, a stochastic decision process can determine a successful load shedding strategy. The stochastic decision process uses the number of untrusted nodes detected to estimate the number of nodes that are attacked by the adversary but not detected with 98% or greater probability.

For example, if the SPS detected 10 untrusted nodes, there is 98.9% probability that there are four or less undetected nodes being attacked by the adversary assuming a normal distribution of undetected attacks on nodes. The stochastic decision process would compensate for this uncertainty by issuing load shedding commands to four additional trusted nodes. In the worst case, there were more than four undetected nodes being attacked by the adversary and the SPS strategy fails to maintain the system stability. In this scenario there is less than a 1.1% probability of this event. Typically, less than four nodes were undetected so a number of the additional load shedding commands results in excess load shedding as evidenced by final frequencies greater than about 58.9 Hz. Best case, there were exactly four undetected nodes and all four additional load shedding commands compensated for the four undetected nodes and resulted in an optimal amount of load shedding. The probability of success used in the SPS's utility function is the probability that the stochastic decision process results in a successful load shedding strategy. The probability of failure in the SPS utility function is the one minus the probability of success.

For the adversary's utility function, the probability of success is determined the same way as the SPS's probability of failure. However, the adversary does not know with certainty how many nodes are being defended by the SPS and develops a strategy with the greatest probability of success given a range of possible numbers of SPS nodes being defended. A goal for the adversary is to attack nodes that are not monitored along with nodes that are monitored. Given the lack of certainty in the SPS detecting the attacks, the attacks on the monitored nodes may then result in the SPS selecting the unmonitored nodes being attacked for the load shedding strategy. In this way, the probability of disrupting the SPS load shedding strategy increases quickly as the SPS monitors fewer nodes. Figure 29 demonstrates how the probability of disrupting the SPS load shedding strategy increases until there is 100% probability of failure if the SPS only defends 17 nodes.

The adversary's probability of attribution provides the restraint on the adversary's attack strategy required so that a defense of the SPS load shedding process is even possible. The concept is also supported by the premise that an adversary possessing the resources to disrupt more SPS nodes will rationally chose not to for fear of repercussion if the attack is attributed to the adversary.

Bibliography

[1] D. Bailey and E. Wright, Practical SCADA for Industry, London: Newnes, 2003.

[2] S. A. Boyer, SCADA: Supervisory Control and Data Acquisition, Research Triangle Park: The Instrument, Systems and Automation Society, 2004.

[3] R. L. Krutz, Securing SCADA Systems, Philidelphia: Wiley Publishing Inc, 2006.

[4] J. Weiss, Protecting Industrial Control Systems From Electronic Threats, New York: Momentum Press, 2010.

[5] M. Grimes, ""SCADA exposed"," in *Proceedings ToorCon 7*, San Diego, CA, 2005.

[6] Office of the President, "Presidential Decision Directive (PDD) 63: Critical Infrastructure Protection," Washington DC, 1998.

[7] Office of the President, "Homeland Securty Policy Directive (HSPD) 7: Critical Infrastructure Identification, Prioritization and Protection," Washington DC, 2008.

[8] K. Zetter, "SCADA System's Hard-Coded Password Circulated Online for Years," 19 July 2010. [Online]. Available: http://www.wired.com/threatlevel/2010/07/siemens-scada/. [Accessed 8 November 2010].

[9] K. Zetter, "Clues Suggest Stuxnet Virus Was Built for Subtle Nuclear Sabotage," 14 November 2010. [Online]. Available: http://www.wired.com/threatlevel/2010/11/stuxnet-clues/. [Accessed 16 November 2010].

[10] E. Barnes, "Mystery Surrounds Cyber Missle That Crippled Iran's Nulcear Weapons Ambitions," 26 11 2010. [Online]. Available: http://www.foxnews.com/scitech/2010/11/26/secret-agent-crippled-irans-nuclear-ambitions/. [Accessed 10 12 2010].

[11] K. Zetter, "Feds' Smart Grid Race Leaves Cybersecurity in the Dust," 28 October 2009. [Online]. Available: http://www.wired.com/threatlevel/2009/10/smartgrid/. [Accessed 11 December 2010].

[12] K. Zetter, "Report: Critical Infrastructures Under Constant Cyberattack Globally," 28 January 2010. [Online]. Available: http://www.wired.com/threatlevel/2010/01/csis-report-on-cybersecurity/. [Accessed 12 December 2010].

[13] K. Zetter, "Simulated Cyberattack Shows Hackers Blasting Away at the Power Grid," 26 September 2007. [Online]. Available: http://www.wired.com/threatlevel/2007/09/simulated-cyber/. [Accessed 11 December 2010].

[14] A. B. MacKenzie and L. A. DaSilva, Game Theory for Wireless Engineers, Morgan & Claypool Publishers, 2006.

[15] M. Kodialam and T. Lakshman, "Detecting Network Intrusions via Samping: A

Game Theoretic Approach," in *IEEE INFOCOM*, San Francisco, 2003.

[16] "Dictionary.com, "cyber," in Dictionary.com Unabridged. Source location: Random House, Inc.," [Online]. Available: http://dictionary.reference.com/browse/cyber. [Accessed 21 January 2012].

[17] D. T. Fahrenkrug, "Cyberspace Defined," [Online]. Available: http://www.au.af.mil/au/awc/awcgate/wrightstuff/cyberspace_defined_wrightstuff_17may07.htm. [Accessed 21 January 2012].

[18] Q. Norton, "Wired.com Threat Level: Anonymous Tricks Bystanders Into Attacking Justice Department," Wired.com, 20 January 2012. [Online]. Available: http://www.wired.com/threatlevel/tag/anonymous/. [Accessed 23 January 2012].

[19] Emirates 24/7, "Emirates 24/7: I Will Finish Israel Off Electronically: Ox-Omar," Emirates 24/7, 22 January 2012. [Online]. Available: http://www.emirates247.com/news/world/i-will-finish-israel-off-electronically-ox-omar-2012-01-22-1.438856. [Accessed 23 January 2012].

[20] M. C. Libicki, Conquest in Cyberspace: National Security and Information Warfare, Cambridge: Cambridge University Press, 2007.

[21] D. Ventre, Information Warfare, Hoboken, NJ: John Wiley & Sons, Inc., 2007.

[22] E. Skoudis and T. Liston, Counter Hack Reloaded: A Ste-by-Step Guide to Computer Attacks and Effective Defenses, Upper Saddle River, NJ: Peasron Education, Inc., 2006.

[23] IBM, "SCADA Whitepaper," July 2007. [Online]. Available: https://www-935.ibm.com/services/us/iss/pdf/scada_whitepaper.pdf. [Accessed 12 December 2010].

[24] R. Patterson, "A Quantum Leap Into the IED Age," in *1996, Rural Electric Power Conference Papers Presented at the 39th Annula Conference*, Fort Worth, TX, 1996.

[25] K. Stouffer, J. Falco and K. Scarfone, "SP 800-82, Guide to Industrial Control (ICS) Systems Security," September 2008. [Online]. Available: http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf. [Accessed 08 November 2010].

[26] A. D. Marshall, "MITRE Technical Report: Addressing Industrial Control Systems in NIST Special Publication 800-53," March 2007. [Online]. Available: http://csrc.nist.gov/groups/SMA/fisma/ics/documents/papers/ICS-in-SP800-53_final_21Mar07.pdf. [Accessed 8 Nov 2010].

[27] D. Maynor and R. Graham, "Maynor-Graham-up.pdf," 23-26 January 2006. [Online]. Available: http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf. [Accessed 12 December 2010].

[28] G. M. Coates, K. Hopkinson, S. Graham and S. H. Kurkowski, "Collaborative, Trust Based Security Mechanisms for a Regional Utility Intranet," *IEEE Transactions on Power Systems,* vol. 23, pp. 831-844, 2008.

[29] D. Proudfoot, "UCA and 61850 for Dummies Siemens Power Transmission and Distribution, 2002. [Online]," 21 March 2002. [Online]. Available:

http://www.nettedautomation.com/download/UCA%20and%2061850%20for%20 dummies%20V12.pdf. [Accessed 11 January 2011].

[30] M. Adamiak, A. Apostolov, M. Begovic, C. Henville, K. Martin, G. Michel, A. Phadke and J. Thorp, "Wide Area Protection-Technology and Infrastructures," *IEEE Transactions on Power Delivery,* vol. 21, no. 2, pp. 601-609, 2006.

[31] C. Bowen, T. Buennemeyer and R. Thomas, "Next generation SCADA security: best practices and client puzzles," in *Proceedings 6th Annual IEEE SMC Information Assurance WOrkshop (IAW)*, West Point, NY, 2005.

[32] S. M. Kaplan, F. Sissine, A. Abel, J. Willington, S. G. Kelly and J. J. Hoecker, Government Series: Smart Grid, Alexandria: The Capitol.Net, 2009.

[33] Department of Energy, "SmartGrid.gov," 11 January 2012. [Online]. Available: http://www.smartgrid.gov/. [Accessed 11 January 2012].

[34] S. M. Kaplan, "Electric Power Transmission: Background and Policy Issues," Congressional Research Service, Washington DC, 2009.

[35] C. W. Gellings, The Smart Grid, Lilburn: The Fairmont Press, 2009.

[36] P. Anderson and B. LeReverend, "Industry Experience with Special Protection Schemes," *IEEE Transactions on Power Systems,* vol. 11, no. 3, pp. 1166-1179, 1996.

[37] P. M. Anderson, Power System Protection, New York: Wiley-Interscience; IEEE Press, 1999.

[38] National Energy Technology Laboratory, "A Vision for the Modern Grid," U.S. Department of Energy, Washington DC, 2007.

[39] P. Kundur, Power System Stability and Control, N. J. Balu and M. G. Lauby, Eds., New York: McGraw-Hill, Inc, 1994.

[40] IEEE Std C37.106-2003 (Revision of ANSI/IEEE C37.106-1987), *IEEE Guide for Abnormal Frequency Protection for Power Generating Plants,* IEEE, 2004, pp. 0_1-34.

[41] D. Berry, R. Brown, J. Redmond and W. Watson, "Underfrequency Protection of the Ontario Hydro System," CIGRE, 1970.

[42] H. Lokay and V. Burtnyk, "Application of Underfrequency Relays for Automatic Load Shedding," *IEEE Transactions,* Vols. PAS-87, pp. 7763-783, 1968.

[43] A. Brown, "SCADA vs. the hackers," 2002. [Online]. Available: http://www.memagazine.org/backissues/membersonly/dec02/features/scadavs/scadavs.html. [Accessed 16 November 2010].

[44] S. P. Marsh, "Formalising Trust as a Computational Concept," 1994.

[45] D. Artz and Y. Gil, "A Survey of Trust in Computer Science and the Semantic Web," *Journal of Web Semantics: Science, Services and Agents on the World Wide Web,* vol. 5, no. 2, pp. 58-71, 2007.

[46] J. F. Kurose and K. W. Ross, Computer Networking: A Top-Down Approach Featuring the Internet, 3rd Edition ed., New York: Pearson Education, Inc., 2005.

[47] S. D. Ramchurn, D. Huynh and N. R. Jennings, "Trust in Multiagent Systems,"

Knowledge Engineering Review, vol. 19, no. 1, pp. 1-25, 2004.

[48] D. Easley and J. Klieinberg, Networks Crowds and Markets, New York: Cambridge University Press, 2010.

[49] H. Li and M. Singhal, "Trust Management in Distributed Systems," *Computer,* pp. 45-53, 2007.

[50] K. M. Hopkinson, K. P. Birman, R. Giovanini, D. V. Coury, X. Wang and J. S. Thorp, "EPOCHS: Integrated Commercial Off-the-Shelf Software for Agent-Based Electric Power and Communications Simulation," in *2003 Winter Simulation Conference*, New Orleans, 2003.

[51] K. Hopkinson, X. Wang, J. T. R. Giovanini, K. Birman and D. Coury, "EPOCHS: A Platform for Agent-based Electric Power and Communications Simulation Built from Commercial Off-The-Shelf Components," *IEEE Transactions on Power Systems,* vol. 21, pp. 548-558, May 2006.

[52] J. Fadul, "Using Reputation Based Trust To Overcome Malfunctions And Malicious Failures In Electrical Power Protections Systems," AFIT, WPAFB (AD-AFIT/DEE/ENG/11-08), 2011.

[53] R. Abe, H. Taoka and D. McQuilken, "Digital Grid: Communicative Electric Grids of the Future," *IEEE Transactions on Smart Grid,* vol. 2, no. 2, pp. 399-410, 2011.

[54] M. Shor, "Game Theory.net - Resources and Teaching Stratedy for Buisness and Life," 2007. [Online]. Available: http://www.gametheory.net/. [Accessed 2 September 2011].

[55] I. Curiel, "Cooperative Combinatorial Games," in *Pareto Optimality, Game Theory, and Equilibrium*, New York, Springer Science+Buisness Media, LLC, 2008, pp. 131-157.

[56] P. Morris, Introduction to Game Theory, New York: Springer-Verlag, 1994.

[57] F. C. Zagare, Game Theory Concepts and Applications, New Park: Sage Publications, 1984.

[58] M. D. Davis, Game Theory:A Non Technical Introduction, New York: Basic Books, Inc, 1970.

[59] L. A. O. Class, K. M. Hopkinson, X. Wang and T. R. Andel, "A Robust Communication-Based Special Protection System," *IEEE Transactions on Power Delivery,* vol. 25, no. 3, pp. 1314-1324, 2010.

[60] U.S.-Canada Power System Outage Task Force and the United States Department of Energy, "Final Report on the August 14, 2003 Blackout in the United States and Canada," U.S. Department of Energy, Washington DC, 2004.

[61] Federal Power Commission, "Report to the President on the Power Failure in the Northeastern United States and the Province of Ontario on Novemeber 9-10, 1965," Federal Power Commission, Washington DC, 1965.

[62] S. McCanne and K. F. S. Floyd, ns2 (network simulator 2), 1989.

[63] R. Jain, The Art of Computer System Performance Analysis: Techniques for

Experimental Design, Measurement, Simulation and Modeling, New York, NY: Wiley-Inter-Science, 1991.

[64] IEEE PES Power Syst. Comm, USA, "Tansient Stability Test Systems for Direct Stability Methods," *IEEE Transactions on Power Systems,* vol. 7, no. 1, pp. 37-43, 1992.

[65] M. Begovic, D. Novosel, D. Karlsson, C. Henville and G. Michel, "Wide-Area Protection and Emergency Control," *Proceeding of the IEEE,* vol. 93, no. 5, pp. 876-891, 2005.

[66] K. Hopkinson, G. Roberts, X. Wang and J. Thorp, "Quality-of-Service Considerations in Utility Communication Networks," *IEEE Transactions on Power Delivery*, vol. 24, no. 3, pp. 1465-1474, 2009.

[67] R. I. Kabacoff, R in Action, Shelter Island, NY: Manning Publications Co., 2011.

[68] S. Shapiro and M. B. Wilk, "An analysis of variance test for normality (complete series)," *Biometrika,* vol. 52, pp. 591-611, 1 December 1965.

[69] P. S. Mann, Intoductory Statistics, Hoboken, NJ: John Wiley and Sons. Inc., 2004.

[70] K. Binmore, Playing for Real: A Text on Game Theory, New York: Oxford University Press, 2007.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 074-0188*

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
22-03-2012	Master's Thesis	August 2010 – March 2012

4. TITLE AND SUBTITLE	**5a. CONTRACT NUMBER**
Application of Game Theory to Improve the Defense of the Smart Grid	**5b. GRANT NUMBER**
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	**5d. PROJECT NUMBER** 12G292P
Ross, Keith J., Captain, USAF	**5e. TASK NUMBER**
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)	**8. PERFORMING ORGANIZATION REPORT NUMBER**
Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way, Building 640 WPAFB OH 45433-8865	AFIT/GCO/ENG/12-10
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Air Force Office of Scientific Research, Mathematics, Information and Life Sciences Directorate Attn : Dr. Robert J. Bonneau 875 N Randolph St, Ste 325, Rm 3112, Arlington, VA 22203 (703) 696-9545 (DSN: 426-9545) Email: robert.bonneau@afosr.af.mil	**10. SPONSOR/MONITOR'S ACRONYM(S)** **AFOSR/NL** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This thesis presents the development and evaluation of a distributed agent based system using reputation based trust and game theoretic techniques to improve the defense of the future smart grid from cyber-attack and equipment malfunctions. Future smart grid capabilities promise to leverage network technologies to revolutionize the production, transmission, distribution and consumption of electrical power. However, the internet like communication also increase the power grid's vulnerability to cyber-attack. This thesis uses simulation linking power systems with communication networks to demonstrate the benefits of a Distributed Decision Making Communication Enable Special Protection System (SPS) using reputation based trust and game theory to protect the power grid from malicious and non-malicious malfunctions. The simulations show that a distributed approach to SPS load shedding successfully maintains power grid stability after an electrical disturbance while using reputation based trust to defend the load shedding from cyber-attack and equipment malfunction. Additional simulations demonstrate the application of game theory to defend the SPS load shedding process when available resources prevent the monitoring and defense of every part of the power grid. The demonstrated capability increases the resiliency of the power grid by preventing uncontrolled blackouts through detection and mitigation of attacks, improving the system's reliability.

15. SUBJECT TERMS

SCADA, Game Theory, Trust Management, Reputation-Based Trust, Cyber Security, Smart Grid, Power Grid

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Kenneth M. Hopkinson, Civ, USAF (ENG)
U	**U**	**U**	**UU**	146	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-6565, ext 4579 (kenneth.hopkinson@afit.edu)